

Received August 9, 2019, accepted August 16, 2019, date of publication August 22, 2019, date of current version September 9, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2936680

# UAV Swarm-Enabled Aerial CoMP: A Physical Layer Security Perspective

XUANXUAN WANG<sup>1,2</sup>, WEI FENG<sup>1,2,3</sup>, (Senior Member, IEEE),  
YUNFEI CHEN<sup>4</sup>, (Senior Member, IEEE), AND NING GE<sup>1,2</sup>, (Member, IEEE)

<sup>1</sup>Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing 100084, China

<sup>2</sup>Department of Electronic Engineering, Tsinghua University, Beijing 100084, China

<sup>3</sup>Peng Cheng Laboratory, Shenzhen 518055, China

<sup>4</sup>School of Engineering, University of Warwick, Coventry CV4 7AL, U.K.

Corresponding author: Wei Feng (fengwei@tsinghua.edu.cn)

This work was supported in part by the Beijing Natural Science Foundation under Grant L172041, in part by the National Natural Science Foundation of China under Grant 61771286, Grant 61701457, and Grant 91638205, and in part by the Beijing Innovation Center for Future Chip.

**ABSTRACT** Unlike aerial base station enabled by a single unmanned aerial vehicle (UAV), aerial coordinated multiple points (CoMP) can be enabled by a UAV swarm. In this case, the management of multiple UAVs is important. This paper considers the power allocation strategy for a UAV swarm-enabled aerial network to enhance the physical layer security of the downlink transmission, where an eavesdropper moves following the trajectory of the swarm for better eavesdropping. Unlike existing works, we use only the large-scale channel state information (CSI) and maximize the secrecy throughput in a whole-trajectory-oriented manner. The overall transmission energy constraint on each UAV and the total transmission duration for all the legitimate users are considered. The non-convexity of the formulated problem is solved by using max-min optimization with iteration. Both the transmission power of desired signals and artificial noise (AN) are derived iteratively. Simulation results are presented to validate the effectiveness of our proposed power allocation algorithm and to show the advantage of aerial CoMP by using only the large-scale CSI.

**INDEX TERMS** Artificial noise, large-scale fading, physical layer security, secrecy throughput, UAV swarm.

## I. INTRODUCTION

In recent years, unmanned aerial vehicles (UAVs) have attracted great interest in wireless communications [1]–[4]. Due to their mobility and elevated position, they can provide agile communications [5]. With their high maneuverability, UAV can augment the network capacity and coverage, especially in the extreme environments without infrastructure, such as disaster rescue, traffic monitoring and so on [1], [6]. More specifically, UAVs are usually cost-effective [7]–[10]. They can be exploited to assist on-demand missions, such as high-speed data transmission in the fifth generation (5G) wireless networks. In addition, with the huge demand in emergency applications, i.e., public safety, delivery and surveillance, deploying a flock of UAVs, or swarm, is becoming more attractive, which plays a vital role in meeting performance requirements for communications between multiple UAVs and 5G [11]–[15].

The associate editor coordinating the review of this article and approving it for publication was Zhen Li.

One of the serious concerns in UAV swarm-enabled aerial networks is how to guarantee the privacy and secrecy of the system. Due to the broadcast nature and inherent randomness of wireless channels, UAV swarm-enabled communication networks are particularly vulnerable to various security threats, such as information eavesdropping, information leakage, data modification and so on. In addition, to facilitate the secure transmission, the UAV swarm often places itself near the legitimate users, which is beneficial to eavesdropping, especially when the eavesdropper moves close to the legitimate users.

## A. RELATED WORK

To achieve perfect security, the conventional encryption schemes are typically implemented at the upper layer using cryptographic methods. However, this is often achieved at the cost of high computational complexity [16].

Unlike the traditional cryptographic methods, physical layer security (PLS), using the information-theoretic and

signal processing approaches, has been widely investigated in the UAV-enabled wireless networks [17]–[20]. They enhance the coverage and security of the wireless systems by exploiting physical characteristics of the wireless channel. Specifically, by adaptively adjusting the UAVs' location, they could overcome the propagation constraints in the cellular systems, and provide new possibilities or opportunities for security enhancement. The authors in [17] utilized UAV as a mobile relay, and maximized the secrecy rate of the system with transmit optimization in a four-node. In [18], the authors investigated UAV-enabled secure communication systems where a mobile UAV sent confidential messages to multiple ground users. By considering the imperfect information on the locations of the eavesdroppers, the authors in [19] investigated a UAV-ground communication system with multiple potential eavesdroppers on the ground. The authors in [20] considered UAV-assisted secure communications between a legitimate transmitter-receiver pair for unknown eavesdropper location by taking UAV as an air-to-ground friendly jammer.

These studies [17]–[20] have provided insightful results for improving the secrecy performance of the UAV-aided wireless communications. However, they assume an ideal free-space path-loss model [17]–[19] between the UAV and the legitimate receivers/eavesdroppers or the instantaneous channel state information (CSI) [20] of the eavesdroppers at the transmitter, which may not be practical.

In practice, it is generally difficult to acquire the instantaneous CSI of the eavesdroppers, especially when they are passive. To deal with that, an effective approach, named as artificial noise (AN), has been proposed to mask the desired signals for enhancing the secrecy performance [21]–[25], where AN is designed based on the instantaneous CSI of the legitimate receiver and transmitted in the null-space of the legitimate channel. Although this scheme is helpful for the security, it requires perfect instantaneous CSI between the source and the legitimate receiver at the transmitter, which is nearly unworkable. The idea is then generalized to the UAV-enabled wireless systems, where a UAV is applied as a mobile jammer to transmit AN [26] or a legitimate receiver [27]. However, these works haven't shown useful guidelines to improve physical layer security of UAV swarm-enabled aerial networks.

## B. MAIN CONTRIBUTIONS

Despite of the above fruitful results, some challenges still remain in the UAV swarm-enabled aerial networks.

For the UAV swarm-enabled aerial networks, an open challenge is how to acquire CSI. To practically depict the typical propagation environments, the composite channel model, consisting of both small-scale and large-scale fading, needs to be used, which is in stark contrast to the existing literatures [17]–[19]. Under the composite channel, one key role for the power allocation strategy is the prior knowledge. Since it is impossible to perfectly acquire the random small-scale fading prior to the whole trajectory of

the UAV swarm, it is almost infeasible to assume perfect CSI. In this paper, we devote to guarantee the secrecy performance of the system in a whole-trajectory-oriented manner by utilizing only the large-scale CSI of the legitimate receivers/eavesdroppers, which can be achieved at much lower cost.

In wireless communication systems, path loss could significantly reduce the signal reception quality at the legitimate users, especially in the UAV swarm-enabled aerial networks. In the existing literatures, one effective scheme to overcome the limitation is by means of multiple antenna systems, i.e., multiple-input single-output (MISO) [28], [29], multiple-input multiple-output (MIMO) [30], [31], or single-input multiple-output (SIMO) [32]. However, due to the limited size, it is hard for UAVs to be equipped with multiple antennas. To handle that, we consider an effective coordinated multiple points (CoMP) between UAVs in this paper, where multiple single-antenna UAVs are combined to form the UAV swarm and then act as a virtual multiple-antenna node. Unlike the conventional CoMP with fixed base stations (BSs), the UAV swarm is able to cooperatively operate as an aerial CoMP by utilizing the mobility of the UAVs. Note that, in contrast to the existing works achieving CoMP based on perfect CSI [33], [34], our scheme uses only the predictable large-scale CSI between UAVs and the legitimate receivers/eavesdroppers.

The transmission energy constraint at each UAV is another challenge for the secrecy performance of UAV swarm-enabled aerial networks. Since it's generally difficult to recharge the battery of the UAV during its flight, not only the transmission power budget but also the total transmission energy constraint should be taken into account for each UAV. Note that the total energy consumption of the UAV consists of two components: the UAV's transmission energy consumption, which is due to the radiation, signal processing as well as other circuitry, and the UAV's propulsion energy consumption, which is determined by the UAV's flying status including the velocity and acceleration [7]. Due to the signal processing of the confidential messages and the circuitry, this work mainly focuses on the transmission energy constraint per UAV.

In addition, the transmission duration used to serve the legitimate users also plays a vital role to improve the secrecy performance of the system. Due to the limited total transmission energy at each UAV, the transmission duration may be restricted, which should be well designed for each legitimate user.

Motivated by the above observations, we investigate the AN-aided secure transmission for the UAV swarm-enabled aerial CoMP, where both of the legitimate receivers and eavesdroppers are equipped with multiple antennas. Different from the conventional eavesdropping, we assume the eavesdropper randomly walks following the trajectory of the UAV swarm, which may significantly deteriorate the secrecy performance of the system. In addition, unlike the existing AN-aided secure transmission based on the instantaneous

CSI of the legitimate users, AN in our proposed scheme is designed by using only the large-scale CSI. To the best of our knowledge, this is the first time that studies AN-assisted secure transmission in the UAV swarm-enabled aerial CoMP by exploiting only the large-scale CSI of the legitimate receivers/eavesdroppers.

Our main contributions of the paper are summarized as follows:

- We consider physical layer security in the UAV swarm-enabled aerial networks. Specifically, multiple single-antenna rotary-wing UAVs perform an aerial CoMP, and enable a virtual MIMO transmission link with the multiple-antenna legitimate receivers or the eavesdropper, in which the swarm transmits the confidential messages in conjunction with AN and sequentially hovers to serve the scheduled legitimate users. Unlike the existing wiretap mode where the eavesdropper keeps static at a fixed location, we consider the eavesdropper moves following the trajectory of the swarm for better eavesdropping in a passive manner.
- To characterize the typical propagation environments, we consider a practical composite channel model consisting of both small-scale and large-scale fading. However, it is infeasible to achieve perfect CSI since the small-scale channel fading is time-varying and hard to be acquired. In this work, we use only the large-scale channel fading, which is more reasonable because the large-scale channel fading mainly depends on the position information of both the UAV and the legitimate receivers/eavesdroppers. We can obtain such information based on the historical data and the related distance between the UAV and the legitimate receivers/eavesdroppers.
- Based on the large-scale CSI, an optimization framework in a whole-trajectory-oriented manner is proposed to maximize the secrecy throughput by jointly optimizing the power allocation between the confidential messages and AN as well as the transmission durations of all the legitimate receivers subject to the overall transmission energy constraint at each rotary-wing UAV. The formulated problem is not convex and hard to be solved directly. To deal with that, an equivalent max-min problem is reformulated by adopting the random matrix theory, and then an efficient iterative algorithm is proposed. Specifically, the problem is split into four subproblems. For the first two and the fourth subproblems, they are convex and can be solved using the general optimization toolbox. For the third subproblem, we first transform its non-convex behavior into the convex one by adopting a successive convex approximation technique. Then, these four subproblems are alternately updated in each iteration. Furthermore, we show that the proposed algorithm guarantees the convergence. Finally, simulation results validate that our proposed scheme could achieve a good secrecy performance.

## C. ORGANIZATION AND NOTATIONS

The rest of the paper is organized as follows. Section II presents the system model and problem formulation. Section III proposes power allocation for secure aerial CoMP. In Section IV, simulation results and discussions are presented. Finally, conclusions are made in Section VI.

Throughout this paper, upper case and lower case boldface letters represent the matrices and the vectors, respectively.  $\mathbf{I}_L$  is an  $L \times L$  identity matrix, and  $\mathbf{0}$  is a zero vector.  $\mathbb{E}(\cdot)$  denotes the expectation operation.  $(\cdot)^H$  and  $\text{Tr}(\cdot)$  represent the conjugate transpose and the trace of a matrix, respectively.  $\mathbf{A} \succeq \mathbf{0}$  denotes that  $\mathbf{A}$  is a positive semidefinite matrix.  $y \sim \mathcal{N}(0, a)$  denotes the Gaussian random variable with mean 0 and variance  $a$ .  $\mathbf{x} \sim \mathcal{CN}(\mathbf{s}, \Sigma)$  is the complex circularly symmetric Gaussian distribution with the mean vector  $\mathbf{s}$  and the covariance matrix  $\Sigma$ .

## II. SYSTEM MODEL AND PROBLEM FORMULATION

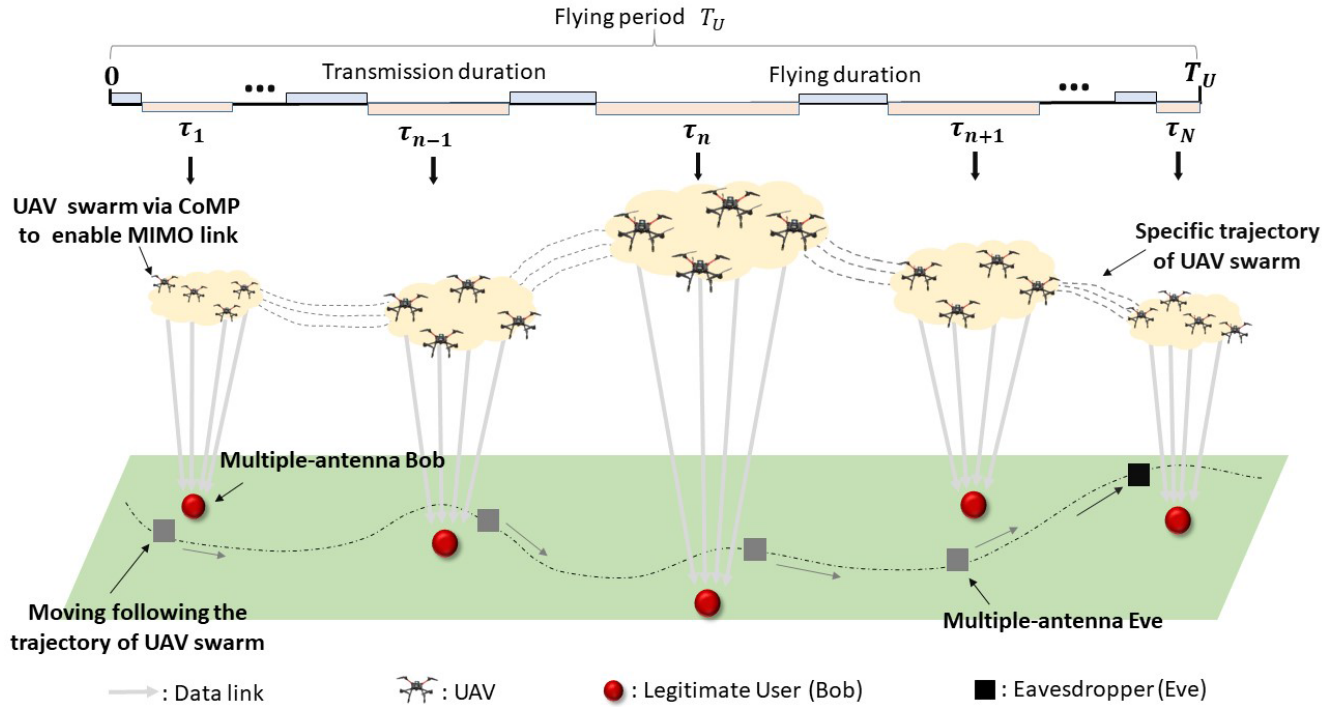
### A. SYSTEM MODEL

We consider the downlink transmission in the UAV swarm-enabled aerial networks. As illustrated in Fig. 1, the system consists of  $L$  rotary-wing UAVs (indexed with  $1, \dots, L$ ),  $N$  legitimate users (indexed with  $1, \dots, N$ ) as Bob, and one eavesdropper as Eve. All the legitimate users and the eavesdropper are equipped with  $N_B$  and  $N_E$  antennas, respectively. For the rotary-wing UAVs, they form a UAV swarm via CoMP, and act as an aerial base station to assist the wireless networks. When the UAVs serve the legitimate users, they are randomly dispatched in a circle centering at the legitimate users with an altitude.

Due to the limited weight and size, only one single antenna is equipped at each UAV. Over the flight of the UAV swarm, the legitimate users could be provided with the confidential messages when being scheduled.<sup>1</sup> Due to the openness of the wireless link, there exists a leakage of the confidential messages. In this system, we assume the eavesdropper is passive and only intends for the confidential messages which are transmitted to the scheduled legitimate users. Furthermore, the eavesdropper randomly moves following the specific trajectory of the swarm to improve eavesdropping. Meanwhile, the eavesdropper also tries to keep a safety distance  $r_e$  away from the scheduled legitimate users so that it could not be spotted.

In this work, we assume the same consecutive period, denoting as  $T_U$ , for each rotary-wing UAV in the swarm, which mainly consists of two parts: the total flying duration  $T_f$  and the total transmission duration  $T_t$ .  $T_f$  is highly dependent on the velocity of the UAVs, and  $T_t$  is determined by the transmission energy consumption of the UAVs. In this work, the UAVs are assumed to serve the scheduled legitimate receivers in a sequential manner. Specifically, they hover above a scheduled legitimate receiver to send the confidential messages during a transmission duration, and then fly to

<sup>1</sup>In fact, the user scheduling issue is important for the system. However, it is out of the scope of this work.



**FIGURE 1.** Illustration of a UAV swarm-enabled aerial network, where a UAV swarm, acting as an aerial CoMP, enables MIMO secure communications with the multiple-antenna legitimate users and the eavesdropper in a whole-trajectory-oriented manner. Specifically, the swarm hovers to serve the scheduled legitimate user in the transmission duration, and then it flies to the next scheduled one within a flying duration. For the eavesdropper, it wiretaps the confidential messages by moving following the trajectory of the UAV swarm.

the next scheduled one within a flying duration. In addition, each legitimate receiver is assumed to be scheduled at most once during the total transmission duration. Denote the transmission durations for the scheduled legitimate users as  $\tau_1, \tau_2, \dots, \tau_N$ , respectively, which change in practice and need to satisfy

$$\sum_{n=1}^N \tau_n \leq T_t, \quad (1)$$

$$0 \leq \tau_n \leq \tau^{\max}, \quad \forall n, \quad (2)$$

where  $\tau^{\max}$  denotes the transmission duration budget. Note that the transmission duration for each scheduled legitimate user is normally short due to the limited transmission energy of the rotary-wing UAV [35].

Suppose that the coordinate of the  $l$ th UAV in the  $n$ th transmission duration is  $(w_l[n], s_l[n], h_l[n])$ ,<sup>2</sup> where  $(w_l[n], s_l[n])$  and  $h_l[n]$  denote the horizontal coordinate and the altitude of the  $l$ th UAV, respectively. Denote the coordinate of the scheduled legitimate user/eavesdropper in the  $n$ th transmission duration as  $(r_q[n], t_q[n], 0)$ , where  $q \in \{B, E\}$ .

<sup>2</sup>The UAVs fly following a specific trajectory, whose locations can be achieved by using the existing positioning technology, i.e., the technology of Global Positioning System (GPS) and BeiDou Navigation Satellite System (BDS) combined positioning [36]. Based on the open channel link, the UAVs can broadcast their locations to legitimate receivers for them to follow.

Thus, the distance between the  $l$ th UAV and  $q$  at the  $n$ th transmission duration is

$$d_{q,l}[n] = \sqrt{(h_l[n])^2 + (w_l[n] - r_q[n])^2 + (s_l[n] - t_q[n])^2}, \quad q \in \{B, E\}. \quad (3)$$

To be practical, we consider both line-of-sight (LoS) and non-line-of-sight (NLoS) connections between the UAVs and the legitimate users. Therefore, the large-scale path loss between the  $l$ th UAV and  $q$  at the  $n$ th transmission duration can be modeled as [37]

$$PL_{q,l}^{dB}[n] = \frac{A}{1 + ae^{-b(\rho_{q,l}[n]-a)}} + B_{q,l}[n], \quad (4)$$

where

$$\begin{aligned} A &= \eta_{\text{LoS}} - \eta_{\text{NLoS}}, \\ B_{q,l}[n] &= 20\lg(d_{q,l}[n]) + 20\lg\left(\frac{4\pi f}{c}\right) + \eta_{\text{NLoS}}, \\ \rho_{q,l}[n] &= \frac{180}{\pi} \arcsin\left(\frac{h_l[n]}{d_{q,l}[n]}\right), \end{aligned}$$

$\eta_{\text{LoS}}$ ,  $\eta_{\text{NLoS}}$ ,  $a$  and  $b$  are constants related to the propagation environment,  $f$  is the carrier frequency, and  $c$  is the speed of light [37].

Consequently, the absolute power loss between the  $l$ th UAV and  $q$  at the  $n$ th transmission duration can be expressed



as:

$$Q_{q,l}[n] = 10^{\frac{\text{PL}_{q,l}[n]}{10}}. \quad (5)$$

The channel from the  $l$ th UAV to  $q$  at the  $n$ th transmission duration can be rewritten as

$$\mathbf{h}_{q,l}[n] = Q_{q,l}^{-\frac{1}{2}}[n] \mathbf{s}_{q,l}[n], \quad (6)$$

where  $\mathbf{s}_{q,l}[n] \in \mathbb{C}^{N_q \times 1}$  represents the small-scale fading between the  $l$ th UAV and  $q$ , of which the entries are independently and identically distributed (i.i.d) according to  $\mathcal{CN}(0, 1)$ .

In order to degrade the eavesdropper's channel, each UAV transmits the confidential message in conjunction with AN. Denoting  $x_l[n]$  as the transmission signal from the  $l$ th UAV to the scheduled legitimate user at the  $n$ th transmission duration, we have

$$x_l[n] = x_l^s[n] + x_l^a[n], \quad (7)$$

where  $x_l^s[n]$  and  $x_l^a[n]$  represent the confidential message and AN from the  $l$ th UAV, respectively.

Furthermore, we express the transmission power from the  $l$ th UAV to the scheduled legitimate user at the  $n$ th transmission duration as

$$\mathbb{E}\{|x_l[n]|^2\} = p_l^s[n] + p_l^a[n], \quad (8)$$

where  $\mathbb{E}\{|x_l^s[n]|^2\} = p_l^s[n]$ ,  $\mathbb{E}\{|x_l^a[n]|^2\} = p_l^a[n]$ ,  $p_l^s[n]$  and  $p_l^a[n]$  denote the power of the confidential message and that of the artificial noise transmitted by the  $l$ th UAV for the scheduled legitimate user at the  $n$ th transmission duration, respectively.

Since each UAV has the limited transmission power, we have

$$0 \leq p_l^s[n] + p_l^a[n] \leq P^{\max}, \quad \forall l, n \quad (9)$$

where (9) represents the transmission power constraint and  $P^{\max}$  is the transmission power budget of each UAV. Considering the short transmission duration, the transmission power is assumed to keep constant at the  $n$ th transmission duration.

Considering the transmission energy limitation of the UAVs within the flying period, the following constraint is achieved

$$\sum_{n=1}^N (p_l^s[n] + p_l^a[n]) \tau_n \leq E^{\max}, \quad \forall l \quad (10)$$

where (10) denotes the total transmission energy constraint at each UAV over the whole flight, and  $E^{\max}$  is the transmission energy budget per UAV.

Based on the aforementioned analysis, all the UAVs work together to transmit the confidential messages for the legitimate users, which could form a virtual  $N_q \times L$  MIMO communication link. Note that to avoid the collision, we assume the UAVs are restricted to fly following their specific trajectory with a minimum safety distance between them. In this case, the composite channel matrix  $\mathbf{H}_q[n] \in \mathbb{C}^{N_q \times L}$  between the

swarm and  $q$  at the  $n$ th transmission duration can be expressed as

$$\mathbf{H}_q[n] = \mathbf{S}_q[n] \mathbf{Q}_q[n], \quad q \in \{B, E\} \quad (11)$$

where

$$\begin{aligned} \mathbf{H}_q[n] &= [\mathbf{h}_{q,1}[n], \mathbf{h}_{q,2}[n], \dots, \mathbf{h}_{q,L}[n]], \\ \mathbf{S}_q[n] &= [\mathbf{s}_{q,1}[n], \mathbf{s}_{q,2}[n], \dots, \mathbf{s}_{q,L}[n]], \\ \mathbf{Q}_q[n] &= \begin{bmatrix} Q_{q,1}^{-\frac{1}{2}}[n] & & \\ & \ddots & \\ & & Q_{q,L}^{-\frac{1}{2}}[n] \end{bmatrix}. \end{aligned}$$

The received signal at the scheduled legitimate user, denoting  $\mathbf{y}_B[n]$ , in the  $n$ th transmission duration, and that at the corresponding eavesdropper, denoting  $\mathbf{y}_E[n]$ , in the  $n$ th transmission duration are given by

$$\mathbf{y}_B[n] = \mathbf{H}_B[n](\mathbf{x}_s[n] + \mathbf{x}_a[n]) + \mathbf{n}_B[n], \quad (12)$$

$$\mathbf{y}_E[n] = \mathbf{H}_E[n](\mathbf{x}_s[n] + \mathbf{x}_a[n]) + \mathbf{n}_E[n], \quad (13)$$

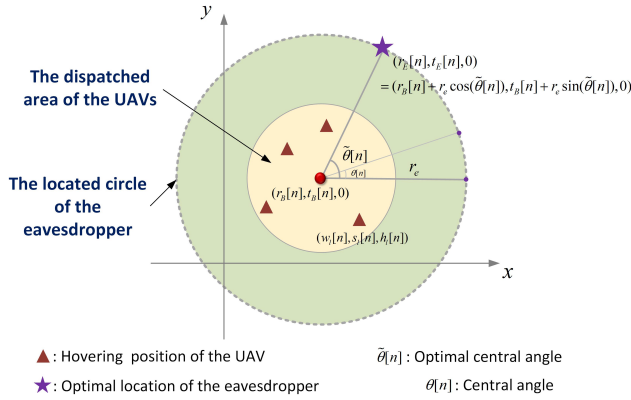
respectively, where  $\mathbf{x}_s[n] \sim \mathcal{CN}(\mathbf{0}, \mathbf{P}_s[n])$  and  $\mathbf{x}_a[n] \sim \mathcal{CN}(\mathbf{0}, \mathbf{P}_a[n])$  denote the confidential messages and AN transmitted by the UAV swarm at the  $n$ th transmission duration,<sup>3</sup> respectively, and  $\mathbf{P}_s[n]$  and  $\mathbf{P}_a[n]$  are their covariance matrices, respectively.  $\mathbf{n}_B[n] \sim \mathcal{CN}(\mathbf{0}, \delta^2 \mathbf{I}_{N_B})$  and  $\mathbf{n}_E[n] \sim \mathcal{CN}(\mathbf{0}, \delta^2 \mathbf{I}_{N_E})$  denote the noise vectors at the scheduled legitimate user and the eavesdropper at the  $n$ th transmission duration, respectively, and  $\delta^2$  represents the noise variance.<sup>4</sup>

*Remark 1:* Note that the locations of the legitimate users/eavesdropper are prior known by the UAV swarm for transmission resource allocation. Specifically, the positions of the legitimate receivers in different transmission durations could be detected by using GPS or Light Detection and Ranging (LiDAR) at the UAVs [40].

Considering the eavesdropper's passive behavior when it randomly follows the specific trajectory of the UAV swarm, it may be difficult to achieve the accurate positions of the eavesdropper at the UAVs. In this work, we consider a worst case scenario, where the power allocation strategy is performed on the assumption that the eavesdropper locates at the optimal position with the strongest receiving power in a circle of radius  $r_e$ . Fig. 2 illustrates the optimal location of the eavesdropper during the  $n$ th transmission duration. Specifically, for the point in the located circle of the eavesdropper with the central angle  $\theta[n]$ , the receiving power from the  $l$ th UAV is  $\frac{p_l^s[n] + p_l^a[n]}{Q_{e,l}[n]} \|\mathbf{s}_{e,l}[n]\|^2$ , where

<sup>3</sup>Different from the existing literatures [38], [39], AN in this work is designed by using only the large-scale CSI instead of the instantaneous legitimate CSI. Owing to the broadcast nature of the wireless channel, AN unavoidably has a leakage and harms the legitimate receivers. Thus, it's important to carefully design the power allocation between the confidential messages and AN so as to minimize the harmful effect on the legitimate users while jamming the eavesdropper, which would be presented in details in the following.

<sup>4</sup>Here, we assume the noise variance is the same, i.e., equal to  $\delta^2$ , over the flying period. For convenience, we drop  $n$  here.



**FIGURE 2.** Illustration of the eavesdropper's optimal location in the located circle of the eavesdropper with the safety distance during the  $n$ th transmission duration (top view of Fig. 1).

$\bar{Q}_{E,l}[n] = Q_{E,l}[n]|_{r_E[n]=r_B[n]+r_e \cos(\theta[n]), t_E[n]=t_B[n]+r_e \sin(\theta[n])}$  based on (5). Considering the constant transmission power in the  $n$ th transmission duration, the optimal central angle can be expressed as  $\tilde{\theta}[n] = \arg \min_{\theta[n] \in [0, 2\pi]} \frac{\bar{Q}_{E,1}[n] + \dots + \bar{Q}_{E,L}[n]}{L}$ . Then, the eavesdropper's optimal location is obtained as  $(r_E[n], t_E[n], 0) = (r_B[n] + r_e \cos(\tilde{\theta}[n]), t_B[n] + r_e \sin(\tilde{\theta}[n]), 0)$ .

## B. PROBLEM FORMULATION

In this subsection, we focus on the problem formulation for this system. Based on (12), the achievable ergodic rate for the scheduled legitimate user at the  $n$ th transmission duration is given by

$$R_B[n] = \mathbb{E}_{\mathbf{S}_B[n]} \left[ \log_2 \det \left( \mathbf{I}_{N_B} + \mathbf{H}_B[n] \mathbf{P}_s[n] (\mathbf{H}_B[n])^H \times \left( \mathbf{H}_B[n] \mathbf{P}_a[n] (\mathbf{H}_B[n])^H + \delta^2 \mathbf{I}_{N_B} \right)^{-1} \right) \right], \quad (14)$$

where  $\mathbb{E}_{\mathbf{S}_B[n]}(\cdot)$  is taken over the random small-scale fading realization of  $\mathbf{S}_B[n]$ ,

$$\mathbf{P}_s[n] = \begin{bmatrix} p_1^s[n] & & \\ & \ddots & \\ & & p_L^s[n] \end{bmatrix}, \quad (15)$$

and

$$\mathbf{P}_a[n] = \begin{bmatrix} p_1^a[n] & & \\ & \ddots & \\ & & p_L^a[n] \end{bmatrix}. \quad (16)$$

Based on (13), the achievable ergodic rate for the eavesdropper who is intended for the confidential message of the scheduled legitimate user at the  $n$ th transmission duration is

$$R_E[n] = \mathbb{E}_{\mathbf{S}_E[n]} \left[ \log_2 \det \left( \mathbf{I}_{N_E} + \mathbf{H}_E[n] \mathbf{P}_s[n] (\mathbf{H}_E[n])^H \times \left( \mathbf{H}_E[n] \mathbf{P}_a[n] (\mathbf{H}_E[n])^H + \delta^2 \mathbf{I}_{N_E} \right)^{-1} \right) \right], \quad (17)$$

where  $\mathbb{E}_{\mathbf{S}_E[n]}(\cdot)$  is taken over the random small-scale fading realization of  $\mathbf{S}_E[n]$ .

Denote  $\Xi = \{\tau_n, \forall n\}$ ,  $\Phi_s = \{\mathbf{P}_s[n], \forall n\}$  and  $\Phi_a = \{\mathbf{P}_a[n], \forall n\}$ . Then, the secrecy throughput for the UAV swarm-enabled aerial networks is defined as [41]

$$R(\Xi, \Phi_s, \Phi_a) = \frac{1}{T_U} \sum_{n=1}^N \tau_n [R_B[n] - R_E[n]]^+, \quad (18)$$

where  $[x]^+ = \max(0, x)$ .

In this work, our goal is to maximize the secrecy throughput over the flying period of the UAV swarm by jointly optimizing the power of the confidential messages (i.e.,  $\Phi_s$ ) and AN power (i.e.,  $\Phi_a$ ) as well as the transmission durations of the legitimate users (i.e.,  $\Xi$ ) under the constraint of the total transmission energy for each UAV. The optimization problem can be formulated as

$$\max_{\Xi, \Phi_s, \Phi_a} \frac{1}{T_U} \sum_{n=1}^N \tau_n [R_B[n] - R_E[n]]^+ \quad (19a)$$

$$\text{s.t. } 0 \leq p_l^s[n] + p_l^a[n] \leq P^{\max}, \quad \forall l, n \quad (19b)$$

$$\sum_{n=1}^N (p_l^s[n] + p_l^a[n]) \tau_n \leq E^{\max}, \quad \forall l \quad (19c)$$

$$\sum_{n=1}^N \tau_n \leq T_t, \quad (19d)$$

$$0 \leq \tau_n \leq \tau^{\max}, \quad \forall n \quad (19e)$$

$$\mathbf{P}_s[n] \geq \mathbf{0}, \quad \forall n, \quad (19f)$$

$$\mathbf{P}_a[n] \geq \mathbf{0}, \quad \forall n. \quad (19g)$$

It can be observed that problem (19) is challenging to be solved for two reasons. First, the operator  $[\cdot]^+$  results in a nonsmooth manner. Second, even without  $[\cdot]^+$ , the objective function (19a) has integrals with the expectation operator  $\mathbb{E}(\cdot)$ , which is intractable and difficult to achieve an explicit expression in terms of  $\Phi_s$ ,  $\Phi_a$  and  $\Xi$ .

*Remark 2:* It is worth mentioning that even though the UAV's propulsion energy is much higher than the UAV's transmission energy [7], we mainly consider the total transmission energy constraint at each UAV in this work. The reasons are as follows:

- (1) Based on (12) - (18), secrecy throughput is highly related to the UAV transmission power consumption. Thus, to maximize the secrecy throughput, the UAV transmission energy consumption is more important than the UAV's propulsion energy consumption.
- (2) We investigate the power allocation strategy to enhance the physical layer security of the downlink transmission in this work, which is part of the process of the signal processing. Based on problem (19), the power mainly denotes the transmission powers of the confidential messages and AN transmitted by the UAVs. Since the propulsion energy is mostly used to keep the UAV aloft as well as support its mobility, it nearly has little contribution to the improvement of the secrecy performance of the system.

(3) We perform the power allocation by considering an optimization framework in a whole-trajectory-oriented manner, where the UAVs follow a specific trajectory. In this case, the UAV's flying status, i.e., the flying period, velocity, propulsion energy consumption and so on, can be controlled with commands from the ground station when they serve the legitimate users/eavesdropper, which leads to the limited consideration of propulsion energy.

### III. POWER ALLOCATION FOR SECURE AERIAL CoMP

In this section, we devote our effort to achieve the optimal solutions of problem (19). Before the further analysis, we first handle the nonsmooth of the objective function in problem (19) by adopting the similar analysis in [19]. Then, (19) can be reformulated into

$$\max_{\Xi, \Phi_s, \Phi_a} \frac{1}{T_U} \sum_{n=1}^N \tau_n [R_B[n] - R_E[n]] \quad (20a)$$

$$\text{s.t. } 0 \leq p_l^s[n] + p_l^a[n] \leq P^{\max}, \quad \forall l, n \quad (20b)$$

$$\sum_{n=1}^N (p_l^s[n] + p_l^a[n]) \tau_n \leq E^{\max}, \quad \forall l \quad (20c)$$

$$\sum_{n=1}^N \tau_n \leq T_I, \quad (20d)$$

$$0 \leq \tau_n \leq \tau^{\max}, \quad \forall n \quad (20e)$$

$$\mathbf{P}_s[n] \geq \mathbf{0}, \quad \forall n, \quad (20f)$$

$$\mathbf{P}_a[n] \geq \mathbf{0}, \quad \forall n, \quad (20g)$$

where problem (20) and problem (19) share the same optimal solution, and  $R(\Xi, \Phi_s, \Phi_a) = \sum_{n=1}^N \frac{\tau_n}{T_U} [R_B[n] - R_E[n]]$ .

To achieve the efficient power allocation, an explicit expression of the objective function in (20) is necessary. Although some works have provided an insightful result to obtain the analytical expression for the objective function, it is generally too cumbersome to do the further power allocation design since the analytical result involves a series of integrals [42].

In the following, we first achieve the closed form of the secrecy throughput in terms of  $\Phi_s$ ,  $\Phi_a$  and  $\Xi$  by removing the expectation operator  $\mathbb{E}(\cdot)$  based on [43]. Then, we reformulate the optimization problem. Finally, a computationally efficient iterative algorithm is proposed for the problem and its convergence is presented.

#### A. PROBLEM TRANSFORMATION

Let  $\mathbf{P}_u[n] = \mathbf{P}_s[n] + \mathbf{P}_a[n], \forall n$ , where  $\mathbf{P}_u[n] = \text{diag}[p_1^u[n], \dots, p_L^u[n]]$ , and  $\Phi_u = \{\mathbf{P}_u[n], \forall n\}$ . Then, the secrecy throughput  $R(\Xi, \Phi_s, \Phi_a)$  can be equivalently rewritten as

$$\begin{aligned} R(\Xi, \Phi_u, \Phi_a) \\ = \frac{1}{T_U} \sum_{n=1}^N \tau_n \left[ \mathbb{E}_{S_B[n]} \left[ \log_2 \det \left( \mathbf{I}_{N_B} + \frac{\mathbf{H}_B[n] \mathbf{P}_u[n] (\mathbf{H}_B[n])^H}{\delta^2} \right) \right] \right. \end{aligned}$$

$$\begin{aligned} & - \mathbb{E}_{S_B[n]} \left[ \log_2 \det \left( \mathbf{I}_{N_B} + \frac{\mathbf{H}_B[n] \mathbf{P}_a[n] (\mathbf{H}_B[n])^H}{\delta^2} \right) \right] \\ & - \mathbb{E}_{S_E[n]} \left[ \log_2 \det \left( \mathbf{I}_{N_E} + \frac{\mathbf{H}_E[n] \mathbf{P}_u[n] (\mathbf{H}_E[n])^H}{\delta^2} \right) \right] \\ & + \mathbb{E}_{S_E[n]} \left[ \log_2 \det \left( \mathbf{I}_{N_E} + \frac{\mathbf{H}_E[n] \mathbf{P}_a[n] (\mathbf{H}_E[n])^H}{\delta^2} \right) \right] \Big]. \end{aligned} \quad (21)$$

It can be observed that (21) is still intractable due to the expectation operator  $\mathbb{E}(\cdot)$ . To cope with that, we try to approximate (21) by introducing the following theorem.

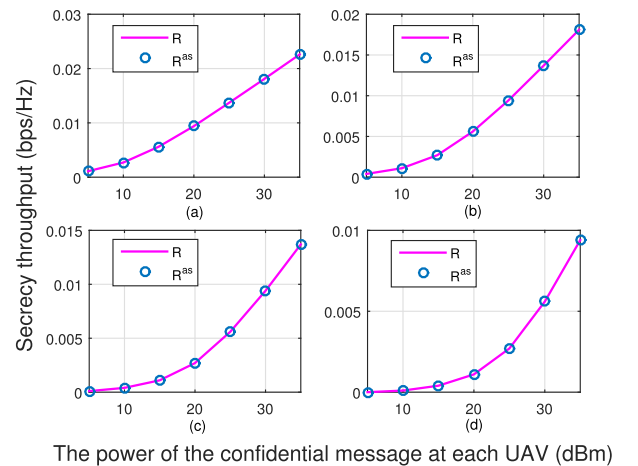
**Theorem 1:** By introducing auxiliary variables  $\mathbf{t}_{B,u} = \{t_{B,u}[n], \forall n\}$ ,  $\mathbf{t}_{E,a} = \{t_{E,a}[n], \forall n\}$ ,  $\mathbf{t}_{B,a} = \{t_{B,a}[n], \forall n\}$ ,  $\mathbf{t}_{E,u} = \{t_{E,u}[n], \forall n\}$ ,  $R(\Xi, \Phi_u, \Phi_a)$  in (21) can be equivalently expressed as

$$\begin{aligned} R^{as}(\Xi, \Phi_u, \Phi_a) = \max_{\mathbf{t}_{B,a} \geq \mathbf{0}, \mathbf{t}_{E,u} \geq \mathbf{0}} \min_{\mathbf{t}_{B,u} \geq \mathbf{0}, \mathbf{t}_{E,a} \geq \mathbf{0}} \\ \mathcal{G}(\Xi, \Phi_u, \Phi_a, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}, \mathbf{t}_{E,u}, \mathbf{t}_{E,a}), \end{aligned} \quad (22)$$

where  $\mathcal{G}(\Xi, \Phi_u, \Phi_a, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}, \mathbf{t}_{E,u}, \mathbf{t}_{E,a})$  is defined in (23) on the top of the next page. Furthermore,  $\mathcal{G}(\Xi, \Phi_u, \Phi_a, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}, \mathbf{t}_{E,u}, \mathbf{t}_{E,a})$  is convex in terms of  $(\mathbf{t}_{B,u}, \mathbf{t}_{E,a})$ , and concave with respect to  $(\mathbf{t}_{B,a}, \mathbf{t}_{E,u})$ .

*Proof:* Please refer to Appendix.  $\square$

Note that the performance gap between  $R(\Xi, \Phi_u, \Phi_a)$  in (21) and  $R^{as}(\Xi, \Phi_u, \Phi_a)$  in (22) is negligible, which has been demonstrated in Fig. 3. Without loss of generality, we randomly select a system topology, and adopt the values of simulation settings in Section IV with different transmission powers based on urban scenario. Specifically, we first verify that  $\mathcal{K}(\Xi, \Phi_u, \Phi_a, \mathbf{w}_{B,u}, \mathbf{w}_{B,a}, \mathbf{w}_{E,u}, \mathbf{w}_{E,a}) = y(\Xi, \Phi_u, \mathbf{w}_{B,u}) - y(\Xi, \Phi_a, \mathbf{w}_{B,a}) - y(\Xi, \Phi_u, \mathbf{w}_{E,u}) + y(\Xi, \Phi_a, \mathbf{w}_{E,a})$ , which is based on the definition (44) in Appendix, is the closed form of  $R(\Xi, \Phi_u, \Phi_a)$  by simulation in Fig. 3. Then, considering the relationship between



**FIGURE 3.** Illustration of the approximate accuracy of  $R^{as}(\Xi, \Phi_u, \Phi_a)$  with the power of the confidential message at each UAV, where we set  $N_B = 5$ ,  $N_E = 3$  and  $L = 7$ . We specify  $\mathbf{P}_a[n] = p_a \mathbf{I}_L, \forall n$  as the input AN power. Particularly,  $p_a$  from (a) - (d) in the figure are set 5dBm, 10dBm, 15dBm, 20dBm, respectively.

$$\begin{aligned}
& \mathcal{G}(\Xi, \Phi_u, \Phi_a, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}, \mathbf{t}_{E,u}, \mathbf{t}_{E,a}) \\
&= \frac{1}{T_U} \sum_{n=1}^N \tau_n \left[ g(\mathbf{P}_u[n], N_B, \mathbf{Q}_B[n], t_{B,u}[n]) - g(\mathbf{P}_a[n], N_B, \mathbf{Q}_B[n], t_{B,a}[n]) \right. \\
&\quad \left. - g(\mathbf{P}_u[n], N_E, \mathbf{Q}_E[n], t_{E,u}[n]) + g(\mathbf{P}_a[n], N_E, \mathbf{Q}_E[n], t_{E,a}[n]) \right] \\
&= \frac{1}{T_U} \sum_{n=1}^N \tau_n \left\{ \left[ \log_2 \det \left( \mathbf{I}_L + \frac{N_B \mathbf{Q}_B[n] \mathbf{P}_u[n] \mathbf{Q}_B[n]}{\delta^2 e^{t_{B,u}[n]}} \right) + N_B \log_2 e(t_{B,u}[n] - 1 + e^{-t_{B,u}[n]}) \right] \right. \\
&\quad - \left[ \log_2 \det \left( \mathbf{I}_L + \frac{N_B \mathbf{Q}_B[n] \mathbf{P}_a[n] \mathbf{Q}_B[n]}{\delta^2 e^{t_{B,a}[n]}} \right) + N_B \log_2 e(t_{B,a}[n] - 1 + e^{-t_{B,a}[n]}) \right] \\
&\quad - \left[ \log_2 \det \left( \mathbf{I}_L + \frac{N_E \mathbf{Q}_E[n] \mathbf{P}_u[n] \mathbf{Q}_E[n]}{\delta^2 e^{t_{E,u}[n]}} \right) + N_E \log_2 e(t_{E,u}[n] - 1 + e^{-t_{E,u}[n]}) \right] \\
&\quad \left. + \left[ \log_2 \det \left( \mathbf{I}_L + \frac{N_E \mathbf{Q}_E[n] \mathbf{P}_a[n] \mathbf{Q}_E[n]}{\delta^2 e^{t_{E,a}[n]}} \right) + N_E \log_2 e(t_{E,a}[n] - 1 + e^{-t_{E,a}[n]}) \right] \right\}. \quad (23)
\end{aligned}$$

$\mathcal{K}(\Xi, \Phi_u, \Phi_a, \mathbf{w}_{B,u}, \mathbf{w}_{B,a}, \mathbf{w}_{E,u}, \mathbf{w}_{E,a})$  and  $\mathcal{G}(\Xi, \Phi_u, \Phi_a, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}, \mathbf{t}_{E,u}, \mathbf{t}_{E,a})$  according to the derivation (52) in Appendix, it is obvious to see that  $R^{as}(\Xi, \Phi_u, \Phi_a)$  is a very accurate approximation for  $R(\Xi, \Phi_u, \Phi_a)$ . In this case, the optimization problem (20) can be reformulated as

$$\begin{aligned}
& \max_{\Xi, \Phi_u, \Phi_a, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}, \mathbf{t}_{E,u}, \mathbf{t}_{E,a}} \min_{\mathbf{t}_{B,u}, \mathbf{t}_{B,a}, \mathbf{t}_{E,u}, \mathbf{t}_{E,a}} \mathcal{G}(\Xi, \Phi_u, \Phi_a, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}, \mathbf{t}_{E,u}, \mathbf{t}_{E,a}) \quad (24a)
\end{aligned}$$

$$\text{s.t.} \quad 0 \leq p_l^u[n] \leq P^{\max}, \quad \forall l, n \quad (24b)$$

$$\sum_{n=1}^N p_l^u[n] \tau_n \leq E^{\max}, \quad \forall l \quad (24c)$$

$$\sum_{n=1}^N \tau_n \leq T_t, \quad (24d)$$

$$0 \leq \tau_n \leq \tau^{\max}, \quad \forall n \quad (24e)$$

$$\mathbf{P}_u[n] - \mathbf{P}_a[n] \geq \mathbf{0}, \quad \forall n, \quad (24f)$$

$$\mathbf{P}_a[n] \geq \mathbf{0}, \quad \forall n, \quad (24g)$$

$$\mathbf{t}_{B,a} \geq \mathbf{0}, \quad \mathbf{t}_{E,u} \geq \mathbf{0}, \quad (24h)$$

$$\mathbf{t}_{B,u} \geq \mathbf{0}, \quad \mathbf{t}_{E,a} \geq \mathbf{0}. \quad (24i)$$

It's worth mentioning that by performing a serial of reformulations, problem (24) is equivalent to the original problem (19). In the following, we devote to an efficient optimization algorithm for the equivalent problem (24).

## B. AN ITERATIVE ALGORITHM TO SOLVE THE PROBLEM

Note that since (24) is not convex, it's generally difficult to achieve the global optimal solutions. In this subsection, we propose an efficient iterative algorithm by adopting the block coordinate descent method to find the stationary solutions of (24). We first decouple the optimization variables into the following four blocks  $(\mathbf{t}_{B,u}, \mathbf{t}_{E,a})$ ,  $(\mathbf{t}_{B,a}, \mathbf{t}_{E,u})$ ,  $(\Phi_u, \Phi_a)$ ,  $\Xi$  and then alternately optimize these four blocks one by one by taking the other variables as the constants obtained in the last iteration. Specifically, for any given transmission power indicators  $(\Phi_u, \Phi_a)$  and the transmission duration

$\Xi$ , the auxiliary variables  $(\mathbf{t}_{B,u}, \mathbf{t}_{E,a})$  (or  $(\mathbf{t}_{B,a}, \mathbf{t}_{E,u})$ ) can be efficiently solved through standard algorithm [44]. For any obtained auxiliary variables  $(\mathbf{t}_{B,a}, \mathbf{t}_{E,u})$  and  $(\mathbf{t}_{B,u}, \mathbf{t}_{E,a})$  as well as the transmission duration  $\Xi$ , the transmission power indicators  $(\Phi_u, \Phi_a)$  can be optimized by the successive convex approximation technique. Finally, the transmission duration  $\Xi$  can be achieved based on the obtained  $(\mathbf{t}_{B,u}, \mathbf{t}_{E,a})$ ,  $(\mathbf{t}_{B,a}, \mathbf{t}_{E,u})$  and  $(\Phi_u, \Phi_a)$ .

Denote  $m \geq 1$  as the number of the iteration step. Problem (24) can be separated into the following four subproblems.

(1) The auxiliary variables  $(\mathbf{t}_{B,u}, \mathbf{t}_{E,a})$

In the  $m$ th iteration, we first optimize  $(\mathbf{t}_{B,u}, \mathbf{t}_{E,a})$  with  $(\Phi_u^{m-1}, \Phi_a^{m-1})$  and  $\Xi^{m-1}$  obtained in the  $m-1$ th iteration. In this case, problem (24) can be reformulated into

$$\begin{aligned}
& \min_{\mathbf{t}_{B,u}, \mathbf{t}_{E,a}} \frac{1}{T_U} \sum_{n=1}^N \tau_n^{m-1} \left[ g(\mathbf{P}_u^{m-1}[n], N_B, \mathbf{Q}_B[n], t_{B,u}[n]) \right. \\
&\quad \left. + g(\mathbf{P}_a^{m-1}[n], N_E, \mathbf{Q}_E[n], t_{E,a}[n]) \right] \quad (25a)
\end{aligned}$$

$$\text{s.t.} \quad \mathbf{t}_{B,u} \geq \mathbf{0}, \quad \mathbf{t}_{E,a} \geq \mathbf{0}. \quad (25b)$$

Based on Theorem 1, we know that problem (25) is convex, which can be efficiently solved by means of the standard optimization toolbox, i.e., CVX.

(2) The auxiliary variables  $(\mathbf{t}_{B,a}, \mathbf{t}_{E,u})$

Based on the obtained  $(\Phi_u^{m-1}, \Phi_a^{m-1})$  and  $\Xi^{m-1}$  in the  $m-1$ th iteration, the variables  $(\mathbf{t}_{B,a}, \mathbf{t}_{E,u})$  can be achieved by

$$\begin{aligned}
& \min_{\mathbf{t}_{B,a}, \mathbf{t}_{E,u}} \frac{1}{T_U} \sum_{n=1}^N \tau_n^{m-1} \left[ g(\mathbf{P}_a^{m-1}[n], N_B, \mathbf{Q}_B[n], t_{B,a}[n]) \right. \\
&\quad \left. + g(\mathbf{P}_u^{m-1}[n], N_E, \mathbf{Q}_E[n], t_{E,u}[n]) \right] \quad (26a)
\end{aligned}$$

$$\text{s.t.} \quad \mathbf{t}_{B,a} \geq \mathbf{0}, \quad \mathbf{t}_{E,u} \geq \mathbf{0}. \quad (26b)$$

which is convex and can be directly solved using CVX.



(3) The transmission power indicators ( $\Phi_u, \Phi_a$ )

The variables ( $\Phi_u, \Phi_a$ ) with the obtained ( $\mathbf{t}_{B,u}^m, \mathbf{t}_{E,a}^m$ ), ( $\mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m$ ) and  $\Xi^{m-1}$  in the  $m$ th iteration can be achieved by solving the following problem

$$\begin{aligned} \max_{\Phi_u, \Phi_a} \quad & \frac{1}{T_U} \sum_{n=1}^N \tau_n^{m-1} \left[ g(\mathbf{P}_u[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,u}^m[n]) \right. \\ & - g(\mathbf{P}_a[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,a}^m[n]) \\ & - g(\mathbf{P}_u[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,u}^m[n]) \\ & \left. + g(\mathbf{P}_a[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,a}^m[n]) \right] \quad (27a) \end{aligned}$$

$$\text{s.t.} \quad \sum_{n=1}^N p_l^u[n] \tau_n^{m-1} \leq E^{\max}, \quad \forall l \quad (27b)$$

$$(24b), (24f), (24g). \quad (27c)$$

Note that both  $g(\mathbf{P}_u[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,u}^m[n])$  and  $g(\mathbf{P}_u[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,u}^m[n])$  are concave with respect to  $\mathbf{P}_u[n]$ , and both  $g(\mathbf{P}_a[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,a}^m[n])$  and  $g(\mathbf{P}_a[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,a}^m[n])$  are concave with respect to  $\mathbf{P}_a[n]$  [43]. Thus, the objective function in (27) actually mixes the addition and subtraction of these four concave terms, which is neither concave with respect to  $\Phi_u$  nor concave with respect to  $\Phi_a$ . That is, problem (27) is not convex in terms of  $\Phi_u$  and  $\Phi_a$ .

To overcome the convexity issue, we approximate the second and the third terms of the objective function in (27) to an affine function based on the first-order Taylor expansion.

The gradient of  $g(\mathbf{P}_a[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,a}[n])^5$  can be rewritten as

$$\begin{aligned} \nabla_{\mathbf{P}_a[n]} g(\mathbf{P}_a[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,a}[n]) \\ = \varphi_{B,a}[n] \mathbf{Q}_B[n] (\mathbf{I}_L + \varphi_{B,a}[n] \mathbf{Q}_B[n] \mathbf{P}_a[n] \mathbf{Q}_B[n])^{-1} \mathbf{Q}_B[n] \\ \triangleq \mathcal{F}(\mathbf{P}_a[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,a}[n]), \quad (28) \end{aligned}$$

where  $\varphi_{B,a}[n] = \frac{\log_2 e N_B}{\delta^2 e^{\mathbf{t}_{B,a}[n]}}$ . Thus, the first-order Taylor expansion of  $g(\mathbf{P}_a[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,a}[n])$  at a certain point  $\tilde{\mathbf{P}}_a[n]$  can be expressed as

$$\begin{aligned} g(\mathbf{P}_a[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,a}[n] | \tilde{\mathbf{P}}_a[n]) \\ = g(\tilde{\mathbf{P}}_a[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,a}[n]) \\ + \text{tr}[\mathcal{F}(\tilde{\mathbf{P}}_a[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,a}[n]) (\mathbf{P}_a[n] - \tilde{\mathbf{P}}_a[n])], \quad (29) \end{aligned}$$

where  $g(\tilde{\mathbf{P}}_a[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,a}[n]) = g(\mathbf{P}_a[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,a}[n])|_{\mathbf{P}_a[n]=\tilde{\mathbf{P}}_a[n]}$ . Clearly,  $g(\mathbf{P}_a[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,a}[n] | \tilde{\mathbf{P}}_a[n])$  is a linear function with respect to  $\mathbf{P}_a[n]$ .

Similarly, the gradient of  $g(\mathbf{P}_u[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,u}[n])$  can be rewritten as

$$\begin{aligned} \nabla_{\mathbf{P}_u[n]} g(\mathbf{P}_u[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,u}[n]) \\ = \varphi_{E,u}[n] \mathbf{Q}_E[n] (\mathbf{I}_L + \varphi_{E,u}[n] \mathbf{Q}_E[n] \mathbf{P}_u[n] \mathbf{Q}_E[n])^{-1} \mathbf{Q}_E[n] \\ \triangleq \mathcal{F}(\mathbf{P}_u[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,u}[n]), \quad (30) \end{aligned}$$

<sup>5</sup>For convenience, we drop  $m$ .

where  $\varphi_{E,u}[n] = \frac{\log_2 e N_E}{\delta^2 e^{\mathbf{t}_{E,u}[n]}}$ . Thus, the first-order Taylor expansion of  $g(\mathbf{P}_u[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,u}[n])$  at a certain point  $\tilde{\mathbf{P}}_u[n]$  can be expressed as

$$\begin{aligned} g(\mathbf{P}_u[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,u}[n] | \tilde{\mathbf{P}}_u[n]) \\ = g(\tilde{\mathbf{P}}_u[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,u}[n]) \\ + \text{tr}[\mathcal{F}(\tilde{\mathbf{P}}_u[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,u}[n]) (\mathbf{P}_u[n] - \tilde{\mathbf{P}}_u[n])], \quad (31) \end{aligned}$$

where  $g(\tilde{\mathbf{P}}_u[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,u}[n]) = g(\mathbf{P}_u[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,u}[n])|_{\mathbf{P}_u[n]=\tilde{\mathbf{P}}_u[n]}$ . Clearly,  $g(\mathbf{P}_u[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,u}[n] | \tilde{\mathbf{P}}_u[n])$  is a linear function in terms of  $\mathbf{P}_u[n]$ .

In this case, problem (27) in the  $m$ th iteration can be recast into

$$\begin{aligned} \max_{\Phi_u, \Phi_a} \quad & \frac{1}{T_U} \sum_{n=1}^N \tau_n^{m-1} \left[ g(\mathbf{P}_u[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,u}^m[n]) \right. \\ & - g(\mathbf{P}_a[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,a}^m[n] | \mathbf{P}_a^{m-1}[n]) \\ & - g(\mathbf{P}_u[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,u}^m[n] | \mathbf{P}_u^{m-1}[n]) \\ & \left. + g(\mathbf{P}_a[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,a}^m[n]) \right] \quad (32a) \end{aligned}$$

$$\text{s.t.} \quad \sum_{n=1}^N p_l^u[n] \tau_n^{m-1} \leq E^{\max}, \quad \forall l \quad (32b)$$

$$(24b), (24f), (24g). \quad (32c)$$

Problem (32) is convex in terms of  $\Phi_u$  and  $\Phi_a$ . Therefore, the optimal variables ( $\Phi_u, \Phi_a$ ) can be solved by utilizing the standard optimization toolbox CVX.

(4) The transmission duration  $\Xi$

In the last step of the  $m$ th iteration, we focus on the transmission duration  $\Xi$  with the obtained ( $\mathbf{t}_{B,u}^m, \mathbf{t}_{E,a}^m$ ), ( $\mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m$ ) and ( $\Phi_u^m, \Phi_a^m$ ), which can be achieved by the following optimization problem

$$\begin{aligned} \max_{\Xi} \quad & \frac{1}{T_U} \sum_{n=1}^N \tau_n \left[ g(\mathbf{P}_u^m[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,u}^m[n]) \right. \\ & - g(\mathbf{P}_a^m[n], N_B, \mathbf{Q}_B[n], \mathbf{t}_{B,a}^m[n]) \\ & - g(\mathbf{P}_u^m[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,u}^m[n]) \\ & \left. + g(\mathbf{P}_a^m[n], N_E, \mathbf{Q}_E[n], \mathbf{t}_{E,a}^m[n]) \right] \quad (33a) \end{aligned}$$

$$\text{s.t.} \quad \sum_{n=1}^N p_l^{u,m}[n] \tau_n \leq E^{\max}, \quad \forall l \quad (33b)$$

$$\sum_{n=1}^N \tau_n \leq T_t, \quad (33c)$$

$$0 \leq \tau_n \leq \tau^{\max}, \quad \forall n \quad (33d)$$

which is a convex optimization, and can be solved by adopting the general toolbox.

Based on the above analysis, an overall iterative algorithm for problem (19) can be achieved. Specifically, in each iteration, the original problem (19) can be optimized by alternately

**Algorithm 1** The Proposed Iterative Algorithm for Solving Problem (19)

- 1: **Initialize:** the transmission power  $\Phi_u^0 = [\mathbf{P}_u^0[1], \dots, \mathbf{P}_u^0[N]]$ , the AN power  $\Phi_a^0 = [\mathbf{P}_a^0[1], \dots, \mathbf{P}_a^0[N]]$ , the transmission duration  $\Xi^0 = [\tau_1^0, \tau_2^0, \dots, \tau_N^0]$  and the accuracy  $\epsilon > 0$ . Set  $m = 0$ .
- 2: **repeat**
- 3: Obtain the optimal set  $(\mathbf{t}_{B,u}, \mathbf{t}_{E,a})$  by solving problem (25) with the obtained sets  $(\Phi_u^{m-1}, \Phi_a^{m-1})$  and  $\Xi^{m-1}$ ,
- 4: Obtain the optimal set  $(\mathbf{t}_{B,a}, \mathbf{t}_{E,u})$  by solving problem (26) with the obtained sets  $(\Phi_u^{m-1}, \Phi_a^{m-1})$  and  $\Xi^{m-1}$ ,
- 5: Obtain the optimal set  $(\Phi_u, \Phi_a)$  by solving problem (27) with the obtained sets  $(\mathbf{t}_{B,u}^m, \mathbf{t}_{E,a}^m)$ ,  $(\mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m)$  and  $\Xi^{m-1}$ ,
- 6: Obtain the optimal set  $\Xi$  by solving problem (33) with the obtained sets  $(\mathbf{t}_{B,u}^m, \mathbf{t}_{E,a}^m)$ ,  $(\mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m)$  and  $(\Phi_u^m, \Phi_a^m)$ ,
- 7:  $m - 1 \leftarrow m$ .
- 8: **until** The fractional increase of the objective function is below the threshold  $\epsilon > 0$ .

solving problem (25), problem (26), problem (27) and problem (33) in an iterative manner. The details of the proposed algorithm can be summarized in Algorithm 1.

### C. CONVERGENCE PERFORMANCE ANALYSIS

To analyze the convergence of the proposed algorithm, we present the following Proposition 1.

*Proposition 1: The approximation of the secrecy throughput is monotonically increasing in each iteration, i.e.,*

$$R^{as}(\Xi^m, \Phi_u^m, \Phi_a^m) \geq R^{as}(\Xi^{m-1}, \Phi_u^{m-1}, \Phi_a^{m-1}), \quad (35)$$

which demonstrates the convergence of the proposed algorithm.

*Proof:* Based on the analysis in Section III-B, we could achieve an approximation of  $\mathcal{G}(\Xi, \Phi_u, \Phi_a, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}, \mathbf{t}_{E,u}, \mathbf{t}_{E,a})$  as shown in (34), as shown at the bottom of this page. Recall that any concave function is upper bounded by its first-order Taylor expansion at a given local point [45]. The following upper-bounded expressions hold

$$g(\mathbf{P}_a[n], N_B, \mathbf{Q}_B[n], t_{B,a}[n]) \leq g(\mathbf{P}_a[n], N_B, \mathbf{Q}_B[n], t_{B,a}[n] | \tilde{\mathbf{P}}_a[n]), \quad (36)$$

and

$$g(\mathbf{P}_u[n], N_E, \mathbf{Q}_E[n], t_{E,u}[n]) \leq g(\mathbf{P}_u[n], N_E, \mathbf{Q}_E[n], t_{E,u}[n] | \tilde{\mathbf{P}}_u[n]), \quad (37)$$

where the equalities in (36) and (37) are met when  $\mathbf{P}_a[n] = \tilde{\mathbf{P}}_a[n]$  and  $\mathbf{P}_u[n] = \tilde{\mathbf{P}}_u[n]$ , respectively.

Thus, we could achieve

$$\mathcal{G}(\Xi, \Phi_u, \Phi_a, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}, \mathbf{t}_{E,u}, \mathbf{t}_{E,a}) \geq \tilde{\mathcal{G}}[\Xi, \Phi_u, \Phi_a, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}, \mathbf{t}_{E,u}, \mathbf{t}_{E,a} | (\tilde{\Phi}_u, \tilde{\Phi}_a)], \quad (38)$$

where the equality holds when  $\Phi_u = \tilde{\Phi}_u$  and  $\Phi_a = \tilde{\Phi}_a$ .

Based on the fact (38), we present the convergence of Algorithm 1, as shown next. In the  $m$ th iteration, the optimal solutions  $(\Phi_u^m, \Phi_a^m)$ ,  $(\mathbf{t}_{B,u}^m, \mathbf{t}_{E,a}^m)$ ,  $(\mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m)$  and  $\Xi^m$  can be obtained by Algorithm 1. Based on the properties of the saddle point [44], the following relationship in the  $m$ th iteration holds

$$\tilde{\mathcal{G}}[\Xi^m, \Phi_u^m, \Phi_a^m, \mathbf{t}_{B,u}^m, \mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m, \mathbf{t}_{E,a}^m | (\tilde{\Phi}_u^{m-1}, \tilde{\Phi}_a^{m-1})] \geq \tilde{\mathcal{G}}[\Xi, \Phi_u, \Phi_a, \mathbf{t}_{B,u}^m, \mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m, \mathbf{t}_{E,a}^m | (\tilde{\Phi}_u^{m-1}, \tilde{\Phi}_a^{m-1})]. \quad (39)$$

Let  $\Phi_u = \Phi_u^{m-1}$ ,  $\Phi_a = \Phi_a^{m-1}$  and  $\Xi = \Xi^{m-1}$ . Then, it follows from (39) that

$$\tilde{\mathcal{G}}[\Xi^m, \Phi_u^m, \Phi_a^m, \mathbf{t}_{B,u}^m, \mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m, \mathbf{t}_{E,a}^m | (\tilde{\Phi}_u^{m-1}, \tilde{\Phi}_a^{m-1})]$$

$$\begin{aligned} & \tilde{\mathcal{G}}[\Xi, \Phi_u, \Phi_a, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}, \mathbf{t}_{E,u}, \mathbf{t}_{E,a} | (\tilde{\Phi}_u, \tilde{\Phi}_a)] \\ &= \frac{1}{T_U} \sum_{n=1}^N \tau_n \left[ g(\mathbf{P}_u[n], N_B, \mathbf{Q}_B[n], t_{B,u}[n]) - g(\mathbf{P}_a[n], N_B, \mathbf{Q}_B[n], t_{B,a}[n] | \tilde{\mathbf{P}}_a[n]) \right. \\ & \quad \left. - g(\mathbf{P}_u[n], N_E, \mathbf{Q}_E[n], t_{E,u}[n] | \tilde{\mathbf{P}}_u[n]) + g(\mathbf{P}_a[n], N_E, \mathbf{Q}_E[n], t_{E,a}[n]) \right] \\ &= \frac{1}{T_U} \sum_{n=1}^N \tau_n \left\{ \left[ \log_2 \det \left( \mathbf{I}_L + \frac{N_B \mathbf{Q}_B[n] \mathbf{P}_u[n] \mathbf{Q}_B[n]}{\delta^2 e^{t_{B,u}[n]}} \right) + N_B \log_2 e \left( t_{B,u}[n] - 1 + e^{-t_{B,u}[n]} \right) \right] \right. \\ & \quad \left. - \left[ \log_2 \det \left( \mathbf{I}_L + \frac{N_B \mathbf{Q}_B[n] \tilde{\mathbf{P}}_a[n] \mathbf{Q}_B[n]}{\delta^2 e^{t_{B,a}[n]}} \right) + N_B \log_2 e \left( t_{B,a}[n] - 1 + e^{-t_{B,a}[n]} \right) \right] \right. \\ & \quad \left. + \frac{\log_2 e N_B}{\delta^2 e^{t_{B,a}[n]}} \text{tr} \left( [\mathbf{Q}_B[n] (\mathbf{I}_L + \frac{N_B}{\delta^2 e^{t_{B,a}[n]}} \mathbf{Q}_B[n] \tilde{\mathbf{P}}_a[n] \mathbf{Q}_B[n])^{-1} \mathbf{Q}_B[n]] (\mathbf{P}_a[n] - \tilde{\mathbf{P}}_a[n]) \right) \right] \\ & \quad \left. - \left[ \log_2 \det \left( \mathbf{I}_L + \frac{N_E \mathbf{Q}_E[n] \tilde{\mathbf{P}}_u[n] \mathbf{Q}_E[n]}{\delta^2 e^{t_{E,u}[n]}} \right) + N_E \log_2 e \left( t_{E,u}[n] - 1 + e^{-t_{E,u}[n]} \right) \right] \right. \\ & \quad \left. + \frac{\log_2 e N_E}{\delta^2 e^{t_{E,u}[n]}} \text{tr} \left( [\mathbf{Q}_E[n] (\mathbf{I}_L + \frac{N_E}{\delta^2 e^{t_{E,u}[n]}} \mathbf{Q}_E[n] \tilde{\mathbf{P}}_u[n] \mathbf{Q}_E[n])^{-1} \mathbf{Q}_E[n]] (\mathbf{P}_u[n] - \tilde{\mathbf{P}}_u[n]) \right) \right] \\ & \quad \left. + \left[ \log_2 \det \left( \mathbf{I}_L + \frac{N_E \mathbf{Q}_E[n] \mathbf{P}_a[n] \mathbf{Q}_E[n]}{\delta^2 e^{t_{E,a}[n]}} \right) + N_E \log_2 e \left( t_{E,a}[n] - 1 + e^{-t_{E,a}[n]} \right) \right] \right\}. \quad (34) \end{aligned}$$

$$\geq \bar{\mathcal{G}}[\Xi^{m-1}, \Phi_u^{m-1}, \Phi_a^{m-1}, \mathbf{t}_{B,u}^m, \mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m, \mathbf{t}_{E,a}^m | (\tilde{\Phi}_u^{m-1}, \tilde{\Phi}_a^{m-1})] \\ \stackrel{(a)}{=} \mathcal{G}(\Xi^{m-1}, \Phi_u^{m-1}, \Phi_a^{m-1}, \mathbf{t}_{B,u}^m, \mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m, \mathbf{t}_{E,a}^m), \quad (40)$$

where (a) holds according to the analysis in (38).

According to (22), we know that<sup>6</sup>

$$R^{as}(\Xi^m, \Phi_u^m, \Phi_a^m) \\ = \max_{\mathbf{t}_{B,a}, \mathbf{t}_{E,u}} \min_{\mathbf{t}_{B,u}, \mathbf{t}_{E,a}} \mathcal{G}(\Xi^m, \Phi_u^m, \Phi_a^m, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}, \mathbf{t}_{E,u}, \mathbf{t}_{E,a}) \\ \stackrel{(b)}{=} \min_{\mathbf{t}_{B,u}, \mathbf{t}_{E,a}} \mathcal{G}(\Xi^m, \Phi_u^m, \Phi_a^m, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m, \mathbf{t}_{E,a}) \\ \stackrel{(c)}{\geq} \min_{\mathbf{t}_{B,u}, \mathbf{t}_{E,a}} \bar{\mathcal{G}}[\Xi^m, \Phi_u^m, \Phi_a^m, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m, \mathbf{t}_{E,a} | (\tilde{\Phi}_u^{m-1}, \tilde{\Phi}_a^{m-1})], \quad (41)$$

where step (b) holds since  $(\mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m)$  are the optimal solutions by using Algorithm 1, and step (c) holds due to the first-order Taylor expansion as shown in (38).

Furthermore, we have

$$\bar{\mathcal{G}}[\Xi^m, \Phi_u^m, \Phi_a^m, \mathbf{t}_{B,u}^m, \mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m, \mathbf{t}_{E,a}^m | (\tilde{\Phi}_u^{m-1}, \tilde{\Phi}_a^{m-1})] \\ = \min_{\mathbf{t}_{B,u}, \mathbf{t}_{E,a}} \bar{\mathcal{G}}[\Xi^m, \Phi_u^m, \Phi_a^m, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m, \mathbf{t}_{E,a} | (\tilde{\Phi}_u^{m-1}, \tilde{\Phi}_a^{m-1})]. \quad (42)$$

Thus, according to (22), (40), (41) and (42), it follows that

$$R^{as}(\Xi^m, \Phi_u^m, \Phi_a^m) \\ \geq \bar{\mathcal{G}}[\Xi^m, \Phi_u^m, \Phi_a^m, \mathbf{t}_{B,u}^m, \mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m, \mathbf{t}_{E,a}^m | (\tilde{\Phi}_u^{m-1}, \tilde{\Phi}_a^{m-1})] \\ \geq \mathcal{G}(\Xi^{m-1}, \Phi_u^{m-1}, \Phi_a^{m-1}, \mathbf{t}_{B,u}^m, \mathbf{t}_{B,a}^m, \mathbf{t}_{E,u}^m, \mathbf{t}_{E,a}^m) \\ \stackrel{(d)}{=} \max_{\mathbf{t}_{B,a}, \mathbf{t}_{E,u}} \min_{\mathbf{t}_{B,u}, \mathbf{t}_{E,a}} \mathcal{G}(\Xi^{m-1}, \Phi_u^{m-1}, \Phi_a^{m-1}, \mathbf{t}_{B,u}, \mathbf{t}_{B,a}, \mathbf{t}_{E,u}, \mathbf{t}_{E,a}) \\ \stackrel{(e)}{=} R^{as}(\Xi^{m-1}, \Phi_u^{m-1}, \Phi_a^{m-1}), \quad (43)$$

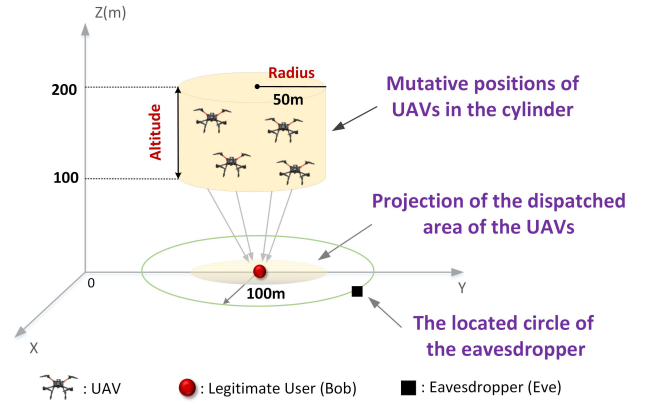
where step (d) holds since  $(\mathbf{t}_{B,u}, \mathbf{t}_{E,a})$  and  $(\mathbf{t}_{B,a}, \mathbf{t}_{E,u})$  are the optimal solutions in Algorithm 1, and step (e) holds according to the closed form of the secrecy throughput in (22).

(43) indicates that  $R^{as}(\Xi, \Phi_u, \Phi_a)$  is nondecreasing in each iteration, which can assure the convergence of Algorithm 1. This completes the proof.  $\square$

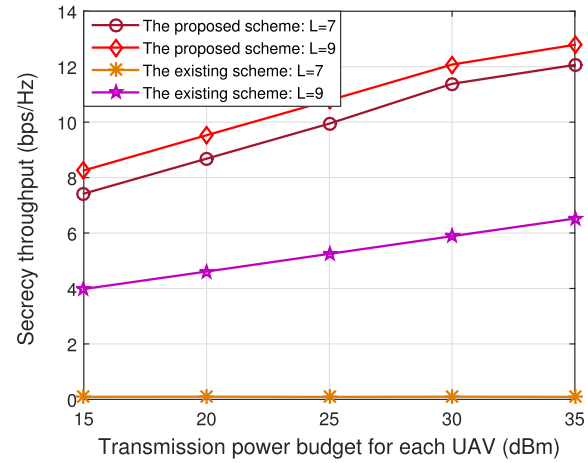
#### IV. NUMERICAL RESULTS AND DISCUSSIONS

In this section, the performance of our proposed scheme is verified by simulation. We consider a  $1000\text{m} \times 1000\text{m}$  square cell, and suppose there are  $N = 10$  legitimate receivers which are randomly distributed in the cell. The multiple single-antenna rotary-wing UAVs, forming a UAV swarm, hover above the scheduled legitimate receiver to provide the confidential messages during a transmission duration. When the UAVs hover to serve the scheduled one, they are randomly dispatched in the circle of radius 50m with altitude  $100\text{m} \sim 200\text{m}$ , which is modeled as a cylinder in Fig. 4. Then, the UAVs fly to the next scheduled one within a flying duration. The eavesdropper randomly locates with a safety distance  $r_e = 100\text{m}$  away from the scheduled legitimate

<sup>6</sup>Due to the limited space, we simplify the constraint  $\mathbf{t}_{q,x} \geq \mathbf{0}$  as  $\mathbf{t}_{q,x}$ , where  $q \in \{B, E\}$  and  $x \in \{u, a\}$ .



**FIGURE 4.** Illustration of positions of UAVs and the eavesdropper during a transmission duration. The UAVs hover at arbitrary positions in the cylinder above the scheduled legitimate user to serve it. The eavesdropper locates in a circle with a safety distance 100m away from the legitimate user.



**FIGURE 5.** Secrecy throughput based on different transmission strategies.

user, which is modeled as a circle in Fig. 4, to hide himself, and moves following the trajectory of the UAV swarm for better eavesdropping. Unless otherwise specified, the system parameters are set as follows: the number of antennas for the legitimate users  $N_B = 5$ , the number of antennas for the eavesdropper  $N_E = 3$ , the transmission duration budget  $\tau^{\max} = 8\text{s}$ , the total transmission duration  $T_t = 100\text{s}$ , the consecutive period  $T_U = 210\text{s}$  [46],  $f = 2.4\text{GHz}$  [4],  $c = 3 \times 10^8\text{m/s}$ ,  $a = 5.0188$ ,  $b = 0.3511$  [37] and the noise covariance  $\delta^2 = -107\text{dBm}$  [43]. The threshold presented in Algorithm 1 is fixed as  $\epsilon = 10^{-3}$ . We consider the typical propagation environments using the following  $(\eta_{\text{LoS}}, \eta_{\text{NLoS}})$  pairs (0.1, 21), (1.0, 20), (1.6, 23), (2.3, 34) corresponding to suburban, urban, dense urban, and highrise urban, respectively [37].

To depict the performance of the proposed scheme, we compare it with the existing scheme in Fig. 5 by considering the suburban environment. We assume  $\mathbf{P}_u^0[n] = \bar{p}_u \mathbf{I}_L, \forall n$ , where  $\bar{p}_u = 20\text{dBm}$ ,  $\mathbf{P}_a^0[n] = \bar{p}_a \mathbf{I}_L, \forall n$ , where  $\bar{p}_a = 10\text{dBm}$ ,  $\Xi^0 = [1, 1, \dots, 1]$ ,  $E^{\max} = 150\text{J}$ . In the existing scheme, confidential messages are transmitted for the legitimate receivers by UAVs, and AN is transmitted in the

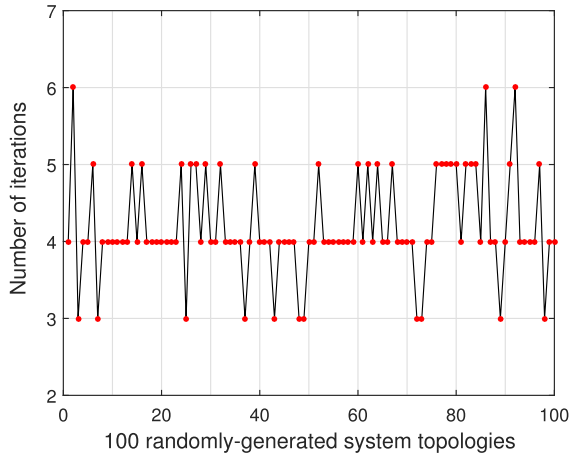


FIGURE 6. Convergence of the proposed algorithm.

null space of the legitimate channel according to the instantaneous CSI  $\mathbf{H}_B$  via precoding. Similar to [39], the power allocation between the desired signals and AN is considered, where the ratio  $\phi = \frac{N_B}{N_E + N_B}$  of the transmission power budget is allocated to the desired signals, and the ratio  $1 - \phi$  is allocated to AN. Note that, this scheme has been widely investigated in the existing literatures but the large-scale CSI has not been taken into account. From the simulation results, we can observe that the proposed scheme presents a significant performance gain over the existing scheme in the case  $L = 7$  and 9, which can be explained as follows. In our proposed scheme, the UAV swarm could adaptively transmit the confidential messages in a higher power when it is close to the legitimate users based on the large-scale CSI, and allocate the higher power for AN when the swarm is close to the eavesdropper, which promotes the secrecy performance improvement. However, due to the inflexible signal transmission mode in the existing scheme, the confidential messages and AN are transmitted in orthogonal channel spaces. Although the eavesdropper can be well suppressed by exploiting AN, it is not able to improve receiving quality of the legitimate receivers with the fixed power of the desired signals. Therefore, a poor secrecy performance is achieved.

To further illustrate the convergence of Algorithm 1, we present the convergence process for 100 randomly-generated system topologies by the proposed Algorithm 1 in the suburban environment in Fig. 6. We initialize  $\mathbf{P}_u^0[n] = \bar{p}_u \mathbf{I}_L$ ,  $\forall n$ , where  $\bar{p}_u = 30\text{dBm}$ ,  $\mathbf{P}_a^0[n] = \bar{p}_a \mathbf{I}_L$ ,  $\forall n$ , where  $\bar{p}_a = 0\text{dBm}$ ,  $\Xi^0 = [1, 1, \dots, 1]$ , and set the transmission power budget  $P^{\max} = 30\text{dBm}$ , the transmission energy budget  $E^{\max} = 300\text{J}$ , the number of the UAVs  $L = 7$ . It can be observed that for the most cases, Algorithm 1 can converge within 6 iterations and the ratio of iterations between  $4 \sim 5$  could achieve 86%, which demonstrates the validity of the proposed scheme.

Fig. 7 illustrates secrecy throughput by Algorithm 1 versus the transmission power budget for each UAV in the suburban scenario. We assume  $\mathbf{P}_u^0[n] = \bar{p}_u \mathbf{I}_L$ ,  $\forall n$ , where  $\bar{p}_u = 20\text{dBm}$ ,  $\mathbf{P}_a^0[n] = \bar{p}_a \mathbf{I}_L$ ,  $\forall n$ , where  $\bar{p}_a = 5\text{dBm}$ ,  $\Xi^0 = [1, 1, \dots, 1]$ ,

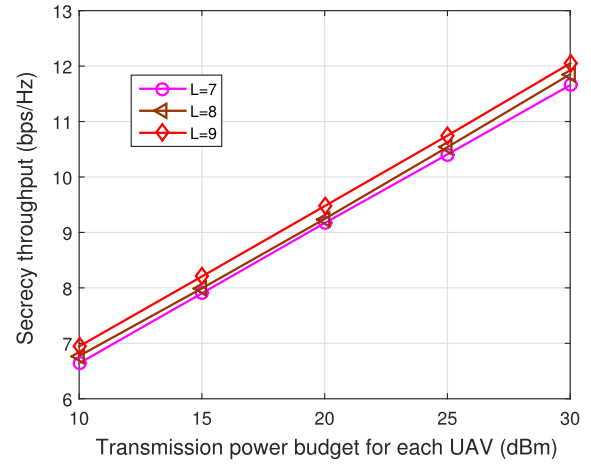


FIGURE 7. Secrecy throughput versus transmission power budget for each UAV.

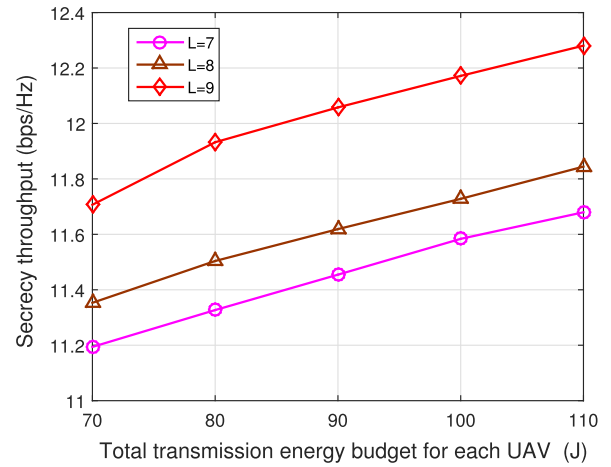
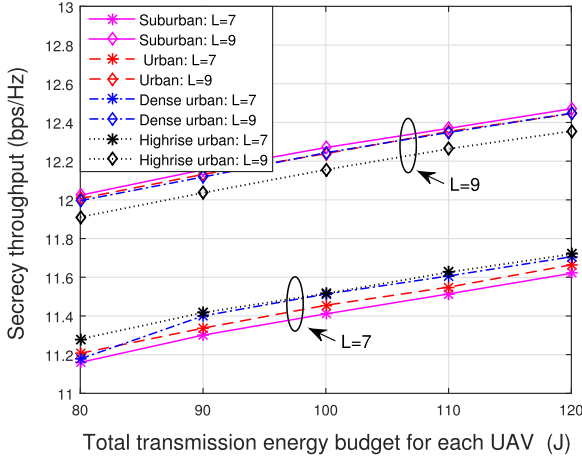


FIGURE 8. Secrecy throughput versus total transmission energy budget for each UAV.

$E^{\max} = 150\text{J}$ . From Fig. 7, we can see that secrecy throughput increases when the transmission power budget for each UAV becomes large. That is due to the fact that the increasing transmission power can enhance the achievable ergodic rate at the legitimate user or the eavesdropper. Furthermore, in our proposed scheme, the confidential message and AN are transmitted independently without cooperation at each UAV. Based on the large-scale CSI, each UAV could allocate more power to the confidential message to improve the achievable rate of Bob when the UAV swarm is close to the legitimate users. When the swarm is close to Eve, more power would be allocated to AN for decreasing the signal receiving quality of Eve. Also, for the same transmission power budget of each UAV, secrecy throughput increases as the number of UAVs in the swarm. Obviously, the larger the number of UAVs is, the higher the power of the confidential messages is, which significantly enhances the secrecy performance of the system.

Fig. 8 depicts secrecy throughput achieved by Algorithm 1 versus the total transmission energy budget for each UAV in the suburban scenario. It is assumed that  $\mathbf{P}_u^0[n] = \bar{p}_u \mathbf{I}_L$ ,  $\forall n$ , where  $\bar{p}_u = 23\text{dBm}$ ,  $\mathbf{P}_a^0[n] = \bar{p}_a \mathbf{I}_L$ ,  $\forall n$ , where





**FIGURE 9.** Secrecy throughput versus total transmission energy budget for each UAV in different typical environments.

$\bar{p}_a = 10\text{dBm}$ ,  $\Xi^0 = [1, 1, \dots, 1]$ , and  $P^{\max} = 35\text{dBm}$ . From Fig. 8, it can be seen that secrecy throughput increases as the total transmission energy constraint for each UAV becomes large. That is because when the transmission energy budget at each UAV increases, the transmission power at each UAV is getting large over its flight. By using the large-scale CSI, the power of the confidential messages and the AN power can be intelligently designed. More power can be transmitted for the confidential messages when the swarm is close to Bob, and more power is allocated for AN when the swarm is near to Eve. Thus, a positive secrecy throughput can be achieved. Furthermore, we can also see that at the same transmission energy budget of each UAV, secrecy throughput grows with the increasing number of UAVs in the swarm. That is due to the fact that as the number of UAVs increases, the total transmission energy of the UAV swarm is getting high. In this case, secrecy throughput could increase.

Fig. 9 presents secrecy throughput obtained by Algorithm 1 versus the total transmission energy budget for each UAV in different urban scenarios. We specify the initial transmission power  $\mathbf{P}_u^0[n] = \bar{p}_u \mathbf{I}_L$ ,  $\forall n$ , where  $\bar{p}_u = 25\text{dBm}$ ,  $\mathbf{P}_a^0[n] = \bar{p}_a \mathbf{I}_L$ ,  $\forall n$ , where  $\bar{p}_a = 10\text{dBm}$ ,  $P^{\max} = 35\text{dBm}$  and  $\Xi^0 = [1, 1, \dots, 1]$ . It can be observed that secrecy throughput is various in the different propagation environments. That comes from that the power loss is highly dependent on the practical urban environments [37], which leads to the divergence of secrecy throughput. Also, it can be seen that as the total transmission energy budget for each UAV becomes large, secrecy throughput increases. Furthermore, secrecy throughput in the case  $L = 9$  is larger than that in the case  $L = 7$ . That is because that the total transmission energy of the UAV swarm increases with the number of UAVs, which leads to the higher secrecy throughput.

## V. CONCLUSIONS

In this paper, we investigated power allocation of AN-assist secure transmission for the UAV swarm-enabled aerial CoMP, where the eavesdropper moved following the

trajectory of the swarm for better eavesdropping. We took the composite channel including small-scale and large-scale fading into account. Considering the hardness in acquiring the perfect CSI, we maximized secrecy throughput by utilizing only the large-scale CSI of the legitimate receivers and the eavesdropper. Specifically, we designed the problem by jointly optimizing the transmission power of the desired signals and the AN power under the constraints of the total transmission energy of each rotary-wing UAV during its flying period and the transmission durations for all the legitimate users. The formulated problem was a non-convex one. To handle that, we first achieved a closed form of the secrecy throughput, and then provided an iterative algorithm for the problem. Finally, we evaluated the effectiveness of our proposed iterative algorithm by means of simulation results.

While an efficient power allocation scheme has been developed to enhance the secure transmission for the UAV swarm-enabled aerial CoMP, in future works we plan to consider a pre-processing framework for the UAV swarm-enabled aerial networks, where the user scheduling, UAV trajectory and UAV altitude will be jointly considered, in order to provide guidelines for the secure design of the system. Furthermore, we will also develop a novel power allocation method based on [47]–[50] by simultaneously considering the blockage caused by the abundant transmission and the transmission energy constraint to improve the secrecy performance of the system.

## APPENDIX PROOF OF THEOREM 1

Considering the identical structure of four terms in (21), we focus on the first term and denote it as  $f_{B,u}(\Xi, \Phi_u) = \frac{1}{T_U} \sum_{n=1}^N \tau_n \mathbb{E}_{S_B[n]} \left[ \log_2 \det \left( \mathbf{I}_{N_B} + \frac{\mathbf{H}_B[n] \mathbf{P}_u[n] (\mathbf{H}_B[n])^H}{\delta^2} \right) \right]$  for clarity. Referring to the remarkable studies in [43], [51], the closed form of  $f_{B,u}(\Xi, \Phi_u)$  could be expressed as

$$\begin{aligned} f_{B,u}(\Xi, \Phi_u) &\approx \frac{1}{T_U} \sum_{n=1}^N \tau_n \left[ \log_2 \det \left( \mathbf{I}_L + \frac{N_B \mathbf{Q}_B[n] \mathbf{P}_u[n] \mathbf{Q}_B[n]}{\delta^2 w_{B,u}[n]} \right) \right. \\ &\quad \left. + N_B \left[ \log_2(w_{B,u}[n]) - \log_2 e \left( 1 - \frac{1}{w_{B,u}[n]} \right) \right] \right] \\ &\triangleq y(\Xi, \Phi_u, \mathbf{w}_{B,u}), \end{aligned} \quad (44)$$

where  $\mathbf{w}_{B,u} = \{w_{B,u}[n] \geq 1, \forall n\}$ , and  $w_{B,u}[n], \forall n$  can be uniquely determined by the following fixed-point equation

$$w_{B,u}[n] = 1 + \sum_{l=1}^L \frac{p_l^u[n] Q_{B,l}^{-1}[n]}{\delta^2 + N_B p_l^u[n] (Q_{B,l}[n] w_{B,u}[n])^{-1}}, \quad \forall n. \quad (45)$$

Note that  $y(\Xi, \Phi_u, \mathbf{w}_{B,u})$  is a quite accurate form of  $f_{B,u}(\Xi, \Phi_u)$  [43]. However,  $y(\Xi, \Phi_u, \mathbf{w}_{B,u})$  is still intractable since  $w_{B,u}[n], \forall n$  involves the variable  $p_l^u[n], \forall n$ . By introducing  $\mathbf{t}_{B,u} = \{t_{B,u}[n], \forall n\}$  and specifying

$w_{B,u}[n] = e^{t_{B,u}[n]}$ ,  $\forall n$ , we have

$$\begin{aligned} & \tilde{y}(\Xi, \Phi_u, \mathbf{t}_{B,u}) \\ &= \frac{1}{T_U} \sum_{n=1}^N \tau_n \left[ \log_2 \det \left( \mathbf{I}_L + \frac{N_B \mathbf{Q}_B[n] \mathbf{P}_u[n] \mathbf{Q}_B[n]}{\delta^2 e^{t_{B,u}[n]}} \right) \right. \\ & \quad \left. + N_B \log_2 \left( t_{B,u}[n] - 1 + e^{-t_{B,u}[n]} \right) \right] \\ &\triangleq \frac{1}{T_U} \sum_{n=1}^N \tau_n g(\mathbf{P}_u[n], N_B, \mathbf{Q}_B[n], t_{B,u}[n]), \end{aligned} \quad (46)$$

where  $\mathbf{t}_{B,u} \geq \mathbf{0}$  and  $e^{t_{B,u}[n]}$ ,  $\forall n$  needs to satisfy (45).

Based on (46), we first consider the partial derivation of  $\tilde{y}(\Xi, \Phi_u, \mathbf{t}_{B,u})$  with respect to  $t_{B,u}[n]$ , which can be expressed as

$$\begin{aligned} & \frac{\partial \tilde{y}(\Xi, \Phi_u, \mathbf{t}_{B,u})}{\partial t_{B,u}[n]} \\ &= -\frac{\tau_n N_B}{T_U \ln 2} \left[ \sum_{l=1}^L \frac{p_l^u[n] (Q_{B,l}[n] e^{t_{B,u}[n]})^{-1}}{\delta^2 + N_B p_l^u[n] (Q_{B,l}[n] e^{t_{B,u}[n]})^{-1}} \right. \\ & \quad \left. - 1 + e^{-t_{B,u}[n]} \right], \quad \forall n. \end{aligned} \quad (47)$$

Let  $s(t_{B,u}[n]) = \sum_{l=1}^L \frac{p_l^u[n] (Q_{B,l}[n] e^{t_{B,u}[n]})^{-1}}{\delta^2 + N_B p_l^u[n] (Q_{B,l}[n] e^{t_{B,u}[n]})^{-1}} - 1 + e^{-t_{B,u}[n]}$ . Thus, we have

$$\frac{\partial \tilde{y}(\Xi, \Phi_u, \mathbf{t}_{B,u})}{\partial t_{B,u}[n]} \begin{cases} < 0, & s(t_{B,u}[n]) > 0, \\ = 0, & s(t_{B,u}[n]) = 0, \\ > 0, & s(t_{B,u}[n]) < 0. \end{cases} \quad (48)$$

Denote  $\mathbf{s}(\mathbf{t}_{B,u}) = [s(t_{B,u}[1]), \dots, s(t_{B,u}[N])]^T$ . It can be observed from (48) that  $\tilde{y}(\Xi, \Phi_u, \mathbf{t}_{B,u})$  is monotonically decreasing when  $\mathbf{s}(\mathbf{t}_{B,u}) > \mathbf{0}$ ,  $\tilde{y}(\Xi, \Phi_u, \mathbf{t}_{B,u})$  is monotonically increasing when  $\mathbf{s}(\mathbf{t}_{B,u}) < \mathbf{0}$ , and  $\tilde{y}(\Xi, \Phi_u, \mathbf{t}_{B,u})$  achieves the extreme minimum point when  $\mathbf{s}(\mathbf{t}_{B,u}) = \mathbf{0}$ . That is, when  $\mathbf{t}_{B,u}$  increases from  $\mathbf{0}$  to infinity, the function  $\tilde{y}(\Xi, \Phi_u, \mathbf{t}_{B,u})$  would first decrease and then increase.

In addition, it can be derived from (47) that

$$\begin{aligned} & \frac{\partial^2 \tilde{y}(\Xi, \Phi_u, \mathbf{t}_{B,u})}{\partial t_{B,u}^2[n]} \\ &= \frac{\tau_n N_B}{T_U \ln 2} \left[ \sum_{l=1}^L \frac{\delta^2 p_l^u[n] Q_{B,l}^{-1}[n] e^{t_{B,u}[n]}}{(\delta^2 e^{t_{B,u}[n]} + N_B p_l^u[n] Q_{B,l}^{-1}[n])^2} + e^{-t_{B,u}[n]} \right] \\ &> 0. \end{aligned} \quad (49)$$

Therefore, we can obtain that

$$\begin{aligned} & \frac{\partial^2 \tilde{y}(\Xi, \Phi_u, \mathbf{t}_{B,u})}{\partial t_{B,u}^2} \\ &= \left[ \frac{\partial^2 \tilde{y}(\Xi, \Phi_u, \mathbf{t}_{B,u})}{\partial t_{B,u}^2[1]}, \dots, \frac{\partial^2 \tilde{y}(\Xi, \Phi_u, \mathbf{t}_{B,u})}{\partial t_{B,u}^2[N]} \right]^T \geq \mathbf{0}, \end{aligned} \quad (50)$$

which indicates that  $\tilde{y}(\Xi, \Phi_u, \mathbf{t}_{B,u})$  is convex in terms of  $\mathbf{t}_{B,u}$ .

With the above discussions from (47) to (50), we can conclude that the function  $\tilde{y}(\Xi, \Phi_u, \mathbf{t}_{B,u})$  would achieve the

minimum value if and only if  $\mathbf{t}_{B,u}$  satisfies the following equation

$$\sum_{l=1}^L \frac{p_l^u[n] (Q_{B,l}[n] e^{t_{B,u}[n]})^{-1}}{\delta^2 + N_B p_l^u[n] (Q_{B,l}[n] e^{t_{B,u}[n]})^{-1}} - 1 + e^{-t_{B,u}[n]} = 0, \quad \forall n. \quad (51)$$

Comparing (45) and (51), it can be observed that when  $\mathbf{t}_{B,u}$  satisfies the fixed-point equation, the function  $y(\Xi, \Phi_u, \mathbf{w}_{B,u})$  would be minimized. Therefore, we have

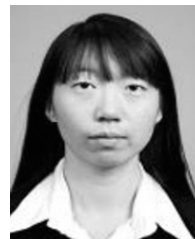
$$y(\Xi, \Phi_u, \mathbf{w}_{B,u}) = \min_{\mathbf{t}_{B,u} \geq \mathbf{0}} \tilde{y}(\Xi, \Phi_u, \mathbf{t}_{B,u}). \quad (52)$$

Finally, we generalize the aforementioned derivation to the other three terms in (21), and then complete the proof.

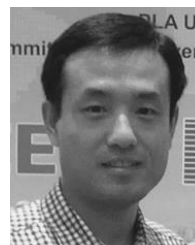
## REFERENCES

- [1] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.
- [2] S. Koulali, E. Sabir, T. Taleb, and M. Azizi, "A green strategic activity scheduling for UAV networks: A sub-modular game perspective," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 58–64, May 2016.
- [3] Y. Zeng, R. Zhang, and T. J. Lim, "Throughput maximization for UAV-enabled mobile relaying systems," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 4983–4996, Dec. 2016.
- [4] X. Wang, W. Feng, Y. Chen, and N. Ge, "Coverage optimization for UAV-aided Internet of Things with partial channel knowledge," *J. Commun. Inf. Netw.*, vol. 3, no. 4, pp. 55–63, Dec. 2018.
- [5] J. Wang, C. Jiang, Z. Han, Y. Ren, R. G. Maunder, and L. Hanzo, "Taking drones to the next level: Cooperative distributed unmanned-aerial-vehicular networks for small and mini drones," *IEEE Veh. Technol. Mag.*, vol. 12, no. 3, pp. 73–82, Sep. 2017.
- [6] C. Yin, Z. Xiao, X. Cao, X. Xi, P. Yang, and D. Wu, "Offline and online search: UAV multiobjective path planning under dynamic urban environment," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 546–558, Apr. 2018.
- [7] Y. Zeng and R. Zhang, "Energy-efficient UAV communication with trajectory optimization," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3747–3760, Jun. 2017.
- [8] Y. Chen, W. Feng, and G. Zheng, "Optimum placement of UAV as relays," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 248–251, Feb. 2018.
- [9] X. Li, W. Feng, Y. Chen, C.-X. Wang, and N. Ge, "Maritime coverage enhancement using UAVs coordinated with hybrid satellite-terrestrial networks," Apr. 2019, *arXiv:1904.02602*. [Online]. Available: <https://arxiv.org/abs/1904.02602>
- [10] T. Qi, W. Feng, and Y. Wang, "Outage performance of non-orthogonal multiple access based unmanned aerial vehicles satellite networks," *China Commun.*, vol. 15, no. 5, pp. 1–8, May 2018.
- [11] Z. Yuan, J. Jin, L. Sun, K.-W. Chin, and G.-M. Muntean, "Ultra-reliable IoT communications with UAVs: A swarm use case," *IEEE Commun. Mag.*, vol. 56, no. 12, pp. 90–96, Dec. 2018.
- [12] B. Li, Z. Fei, and Y. Zhang, "UAV communications for 5G and beyond: Recent advances and future trends," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2241–2263, Apr. 2019.
- [13] *Service Requirements for Next Generation New Services and Markets*, document TS 22.261, Version 15.2.0, 3GPP, Sep. 2017.
- [14] *Feasibility Study on New Services and Markets Technology Enablers for Critical Communications; Stage 1*, document TR 22.862, Version 14.1.0, 3GPP, Oct. 2016.
- [15] *Enhanced LTE Support for Aerial Vehicles*, document TR 36.777, Version 0.3.0, 3GPP, Sep. 2017.
- [16] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1066–1087, 2nd Quart., 2015.
- [17] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 310–313, Jun. 2017.
- [18] H. Lee, S. Eom, J. Park, and I. Lee, "UAV-aided secure communications with cooperative jamming," *IEEE Trans. Veh. Commun.*, vol. 67, no. 10, pp. 9385–9392, Oct. 2018.

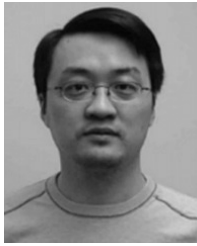
- [19] M. Cui, G. Zhang, Q. Wu, and D. W. K. Ng, "Robust trajectory and transmit power design for secure UAV communications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 9042–9046, Sep. 2018.
- [20] Y. Zhou, P. L. Yeoh, H. Chen, Y. Li, R. Schober, L. Zhuo, and B. Vucetic, "Improving physical layer security via a UAV friendly jammer for unknown eavesdropper location," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11280–11284, Nov. 2018.
- [21] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.
- [22] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.
- [23] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.
- [24] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.
- [25] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.
- [26] X. Zhou, Q. Wu, S. Yan, F. Shu, and J. Li, "UAV-enabled secure communications: Joint trajectory and transmit power optimization," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 4069–4073, Apr. 2019.
- [27] C. Liu, T. Q. S. Quek, and J. Lee, "Secure UAV communication in the presence of active eavesdropper (invited paper)," in *Proc. IEEE Int. Conf. Wireless Commun. Signal Process.*, Nanjing, China, Oct. 2017, pp. 1–6.
- [28] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
- [29] Q. Shi, L. Liu, W. Xu, and R. Zhang, "Joint transmit beamforming and receive power splitting for MISO SWIPT systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3269–3280, Jun. 2014.
- [30] A. Khisti and G. Wornell, "Secure transmission with multiple antennas-part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
- [31] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.
- [32] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Adelaide, SA, Australia, Sep. 2005, pp. 2152–2155.
- [33] S. Mosleh, L. Liu, and J. Zhang, "Proportional-fair resource allocation for coordinated multi-point transmission in LTE-advanced," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5355–5367, Aug. 2016.
- [34] B. Du, C. Pan, W. Zhang, and M. Chen, "Distributed energy-efficient power optimization for CoMP systems with max-min fairness," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 999–1002, Jun. 2014.
- [35] W. Feng, J. Wang, Y. Chen, X. Wang, N. Ge, and J. Lu, "UAV-aided MIMO communications for 5G Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1731–1740, Apr. 2019.
- [36] L. Wang, X. Wen, and C. Huang, "Application of low cost GPS/BDS receiver in UAV precise navigation and positioning," in *Proc. China Satell. Navigation Conf.*, Changsha, China, May 2016, pp. 165–174.
- [37] A. Al-Hourani, S. Kandeepan, and S. Lardner, "Optimal LAP altitude for maximum coverage," *IEEE Wireless Commun. Lett.*, vol. 3, no. 6, pp. 569–572, Dec. 2014.
- [38] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [39] N. Li, X. Tao, H. Wu, J. Xu, and Q. Cui, "Large-system analysis of artificial-noise-assisted communication in the multiuser downlink: Ergodic secrecy sum rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7036–7050, Sep. 2016.
- [40] B. Yang and C. Chen, "Automatic registration of UAV-borne sequent images and LiDAR data," *ISPRS J. Photogramm. Remote Sens.*, vol. 101, pp. 262–274, Mar. 2015.
- [41] Z. Chu, H. X. Nguyen, T. A. Le, M. Karamanoglu, E. Ever, and A. Yazici, "Secure wireless powered and cooperative jamming D2D communications," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 1, pp. 1–13, Mar. 2018.
- [42] L. Hanlen and A. Grant, "Capacity analysis of correlated MIMO channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 11, pp. 6773–6787, Nov. 2012.
- [43] W. Feng, Y. Wang, N. Ge, J. Lu, and J. Zhang, "Virtual MIMO in multi-cell distributed antenna systems: Coordinated transmissions with large-scale CSIT," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2067–2081, Oct. 2013.
- [44] R. Brayton, S. Director, G. Hachtel, and L. Vidigal, "A new algorithm for statistical circuit design based on quasi-Newton methods and function splitting," *IEEE Trans. Circuits Syst.*, vol. CAS-26, no. 9, pp. 784–794, Sep. 1979.
- [45] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
- [46] Q. Wu, Y. Zeng, and R. Zhang, "Joint trajectory and communication design for multi-UAV enabled wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 2109–2121, Mar. 2018.
- [47] S. Li, L. Li, Z. Li, X. Chen, T. Fernando, H. H.-C. Iu, G. He, Q. Wang, and X. Liu, "Event-trigger heterogeneous nonlinear filter for wide-area measurement systems in power grid," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2752–2764, May 2019.
- [48] Y. Yu, Z. Li, X. Liu, K. Hirota, X. Chen, T. Fernando, and H. H.-C. Iu, "A nested tensor product model transformation," *IEEE Trans. Fuzzy Syst.*, vol. 27, no. 1, pp. 1–15, Jan. 2019.
- [49] X. Liu, L. Li, Z. Li, X. Chen, T. Fernando, H. H.-C. Iu, and G. He, "Event-trigger particle filter for smart grids with limited communication bandwidth infrastructure," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6918–6928, Nov. 2018.
- [50] B. Liu, Z. Li, X. Chen, Y. Huang, and X. Liu, "Recognition and vulnerability analysis of key nodes in power grid based on complex network centrality," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 65, no. 3, pp. 346–350, Mar. 2018.
- [51] W. Feng, N. Ge, and J. Lu, "Coordinated satellite-terrestrial networks: A robust spectrum sharing perspective," in *Proc. Wireless Opt. Commun. Conf.*, Newark, NJ, USA, Apr. 2017, pp. 1–5.



**XUANXUAN WANG** received the B.S. degree in communication engineering from Henan Polytechnic University, in 2010, the M.S. degree in electronic and communication engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2013, and the Ph.D. degree from the Institute of Information and Engineering, Chinese Academy of Sciences, China, in 2017. She is currently a Postdoctoral Research Fellow with the Department of Electronic Engineering, Tsinghua University, Beijing. Her current research interests include communication security, UAV-enabled wireless networks, and convex optimization techniques.



**WEI FENG** (S'06–M'10–SM'19) received the B.S. and Ph.D. degrees (Hons.) from the Department of Electronic Engineering, Tsinghua University, Beijing, China, in 2005 and 2010, respectively, where he is currently an Associate Professor. He is also with the Beijing National Research Center for Information Science and Technology, and the Peng Cheng Laboratory. His research interests include maritime broadband communication networks, large-scale distributed antenna systems, and coordinated satellite-UAV-terrestrial networks. He has received the Outstanding Ph.D. Graduate of Tsinghua University Award, in 2010, the IEEE WCSP Best Paper Award, in 2013, the first Prize of Science and Technology Award of China Institute of Communications, in 2015, the IEEE WCSP Best Paper Award, in 2015, the second Prize of National Technological Invention Award of China, in 2016, and the IEEE WOCC Best Paper Award, in 2019. He currently serves as the Assistant to the Editor-in-Chief of *China Communications*, an Editor of the *IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING*, and an Associate Editor of *IEEE ACCESS*.



**YUNFEI CHEN** (S'02–M'06–SM'10) received the B.E. and M.E. degrees in electronic engineering from Shanghai Jiao Tong University, China, in 1998 and 2001, respectively, and the Ph.D. degree from the University of Alberta, Edmonton, AB, Canada, in 2006. He is currently with the School of Engineering, Warwick University, Coventry, U.K. His current research interests include energy harvesting, wireless relaying and general performance analysis, and design of wireless systems.



**NING GE** (M'97) received the B.S. and Ph.D. degrees from Tsinghua University, China, in 1993 and 1997, respectively. From 1998 to 2000, he worked on the development of ATM switch fabric ASIC in ADC Telecommunications, Dallas, TX, USA. Since 2000, he has been with the Department of Electronic Engineering, Tsinghua University. He is currently a Professor and the Director of the Communication Institute. He has published more than 100 articles. His current research interests include communication ASIC design, short range wireless communication, and wireless communications. He is a Senior Member of CIC and CIE.

...